

COUNTY GOVERNMENT OF NYERI



Town Hall - 2nd Floor
Along Kenyatta Road
P.O. Box 1112 - 10100
Telephone 061 2030700
NYERI

Email: nyericountysecretary@gmail.com

OFFICE OF THE COUNTY SECRETARY/HEAD OF COUNTY PUBLIC SERVICE

Ref: CGN/CS/EXTRACTS/VOL. II/101/55

25th August, 2021

Chief Officer
Governor's Office


MINUTE CECM 663/2021: NYERI COUNTY INFORMATION TECHNOLOGY AND COMMUNICATION [ICT] POLICY, 2021

The County Secretary tabled the Nyeri County Information Technology and Communication [ICT] Policy for consideration by Cabinet.

It was proposed by CECM Dr. Rachael Kamau and seconded by CECM James Wachuhi and **resolved: -**

- a) That the Nyeri County Information, Technology and Communication [ICT] Policy, 2021 be and is hereby approved. – **Action – County Secretary**

Certified as true extract of the minutes of the Executive of County Government of Nyeri duly constituted on 23rd August, 2021.


Benjamin W. Gachichio

COUNTY SECRETARY/HEAD OF COUNTY PUBLIC SERVICE

Copy to:

- Ag. Director I.C.T

APPROVAL OF ICT POLICY DOCUMENT

This policy document was discussed and approved for productive use by the Nyeri County Executive on

23rd August, 2021

.....

and therefore comes into force on the date of the approval.

Version 1.0

FOREWORD

In today's rapidly changing technological world, the application of Information Communication Technology (ICT) in organizations and our communities is the order of the day, and developing organizational-wide information systems and networks requires a policy framework. The Kenya's Vision 2030 has placed ICT as one of its key pillars and recognizes the important role ICT plays in the country's development agenda. The Leadership of the County Government of Nyeri recognizes that the world is now a knowledge economy. The importance of ICT in innovation for wealth creation amongst our youth and enhancing service delivery to the people in communities has also been embraced in the County's Integrated Development Plan (CIDP). This realization has reinforced the need for investment in ICT to contribute to the economic development of the county geared towards realization of the Digital Economy Blueprint for the Country at large.

This ICT policy document is geared towards providing a framework for use of ICT in Governance and the realization of best practices and utilization of resources in the County Government in conformity with the existing government policies, legal and regulatory framework and ensure returns from public investment.

The County Government therefore, affirms its commitment to adopt and operationalize this Policy to ensure professionalism, best practices, accountability, transparency, consistency and ethical use of ICT in service delivery by its staff and in engagement with external stakeholders.

The County Government further acknowledges the importance of and shall support ICT utilization in service provision and innovation for the benefit of the government and the people of Nyeri County.

H.E The Governor,

Edward Mutahi Kahiga

ACKNOWLEDGEMENT

We wish to acknowledge the tireless effort put in the realization of this policy through the unwavering support by H.E Hon. Edward Mutahi Kahiga who has always emphasized the need of legal framework in management of ICT in the County Government of Nyeri. We also acknowledge the Contribution of the County Committee Members in coming up with this policy document as well as the Chief Officers, Directors, County ICT team and the entire County staff who took their time to review, critic and amend this ICT Policy.

Benjamin Gachichio

County Secretary

Head of County Public Service.

TABLE OF CONTENTS

APPROVAL OF ICT POLICY DOCUMENT	2
FOREWORD.....	3
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	6
ABBREVIATIONS AND ACRONYMS.....	16
CHAPTER ONE.....	17
1. Introduction.....	17
1.1 ICT Vision, Mission and Core Values	17
1.2 Objectives and Strategies.....	18
1.4 Scope	19
1.5 Purpose.....	19
1.6 Guiding Principles.....	20
1.7 Policy Application.....	21
1.8 Laws and Regulatory Framework	21
1.9 Policy Provisions.....	22
1.10 Policy Compliance and Sustainability	24
1.11 Consequences of non-compliance	24
1.12 Reporting irresponsible or inappropriate use.....	24
1.13 Policy review and practices oversight	25
1.14 Related requirements	25
CHAPTER TWO	26
2. NETWORK SECURITY	26
2.1 Introduction	26
2.2 Policy Statement.....	26
2.3 Environment.....	28
2.4 Configuration and Maintenance	29
2.5 Administration.....	32
2.6 Monitoring and Event Logging	33
2.7 Remote Access	34
CHAPTER THREE	36
3. WIRELESS SECURITY	36
3.1 Introduction	36

3.2	Purpose	36
3.3	Policy Statement.....	37
3.4	Scope	37
3.5	Restrictions.....	37
3.6	Appropriate Use	38
3.7	Regulatory Framework.....	39
3.8	Acceptance	39
3.9	Roles and Responsibilities	39
3.10	User responsibilities	39
CHAPTER FOUR		41
4.	ACCESS CONTROL	41
4.1	Introduction	41
4.2	Authorised Users	41
4.3	Purpose	42
4.4	Scope	42
4.5	Systems and Information Access	42
4.6	Systems and Information De-Registration	43
4.7	Log-On Considerations	44
4.8	Physical Access and Controls	44
4.9	Responsibilities	46
CHAPTER FIVE		48
5.	SERVER ROOM & SERVER SECURITY	48
5.1	Introduction	48
5.2	Purpose	48
5.3	Scope	48
5.4	Policy Statement.....	48
5.5	Server Room Security	48
5.6	Environment.....	50
5.7	Server Configuration and Maintenance.....	50
5.8	Administrative Accounts.....	52
5.9	Service Accounts.....	53
5.10	Remote Access	54
CHAPTER SIX.....		55
6.	PUBLIC INTERNET ACCESS.....	55
6.1	Introduction	55

6.2	Purpose	55
6.3	Scope	55
6.4	Responsibilities	56
6.5	Policy statement	57
6.6	Compliance with the following Public Internet Access Code of Conduct	57
6.7	Legal Framework Governing Public Internet Access	57
6.8	Terms and Conditions	58
7.	THIRD PARTY CONNECTIONS	60
7.1	Introduction	60
7.2	Purpose	60
7.3	Scope	60
7.4	Third Party Compliance	61
7.9	Compliance with other Sections of the ICT policy	64
	CHAPTER EIGHT	65
8.	ICT ASSET MANAGEMENT AND EQUIPMENT USE.....	65
8.1	Introduction	65
8.2	Purpose	65
8.3	Categorise of ICT Assets	66
8.4	Scope	66
8.5	Policy Statement.....	67
8.6	Information and Information Systems	67
8.7	Software	68
8.8	Physical	69
8.9	Services	71
8.10	Personnel	71
8.11	Intangibles	72
8.12	Information Classification	72
8.13	Acceptable Use of Assets	72
8.14	Software: Software Installation	73
8.15	Software Change Control	73
8.16	Reporting of Incidents	74
8.17	Computer Equipment: Protection of ICT Equipment Off-Premises	74
8.18	Equipment Change Control	74
8.19	Transfer of Equipment between Users	74
8.20	Standardisation of Hardware and Software	74

8.21	Loss of ICT equipment	75
8.22	Unattended User Equipment.....	75
8.23	Disposal and Reuse of Equipment.....	76
8.24	ICT Equipment by Category: Critical ICT Equipment	76
8.25	Laptops	77
8.26	Removable Media.....	77
8.27	Printers.....	77
8.28	Personal Use	78
8.31	House Keeping	79
8.32	Movement of ICT Equipment to and from County Government Premises.....	79
8.33	Computer user’s responsibilities	80
8.34	Responsibilities fo The Directorate of ICT	80
CHAPTER NINE.....		81
9.	CYBER SECURITY.....	81
9.1	Introduction	81
9.2	What are we protecting?.....	82
9.3	Classification of Information.....	82
9.4	Classification of Computer Systems	82
9.5	Local Area Network (LAN) Classifications	84
9.6	Definitions.....	84
9.7	Threats to Security	85
9.8	Amateur Hackers and Vandals.....	85
9.9	Criminal Hackers and Saboteurs.....	85
9.10	User Responsibilities	85
9.11	Acceptable Use	86
9.12	User Classification.....	86
9.13	Monitoring Use of Computer Systems	87
9.14	Access Control.....	88
9.15	User System and Network Access – Normal User Identification	88
CHAPTER TEN		89
10.	SERVER SECURITY	89
10.1	Introduction	89
10.2	Purpose	89
10.3	Scope	89
10.4	Policy Statement	89

10.5 Server Room Manager Responsibilities	89
10.6 Environment	91
10.7 Configuration and Maintenance	91
10.8 Administrative Accounts	93
10.9 Service Accounts	94
10.10 Remote Access	94
11. PASSWORD MANAGEMENT	96
11.1 Introduction	96
11.2 Purpose	96
11.3 Scope	96
11.4 Policy Statement	97
11.5 Domain Range	97
11.6 Guidelines	99
11.7 Creating Passwords using Passphrases/Sentences	100
11.8 Password Protection Standards	101
11.9 Additional Information	101
11.10 Application Development Standards	102
CHAPTER TWELVE	102
12. ENCRYPTION	102
12.1 Introduction	102
12.2 Purpose	103
12.3 Scope	103
12.4 Policy Statement	104
12.5 Application	104
12.6 Method	105
12.7 Responsibilities	106
12.8 Use of portable storage media and devices	106
CHAPTER THIRTEEN	108
13. SECURE DESK/DATA PROTECTION	108
13.1 Introduction	108
13.2 Objectives	108
13.3 Key Principles	108
13.4 Definitions	109
13.5 Scope	110
13.6 Responsibilities	110

13.7 Secure Desk Procedure - Protecting Data and Information.....	111
13.8 Electronic Storage Devices.....	112
13.9 Personal Computers, Laptops and Personal Digital Assistants.	112
13.10 Printers, Photocopiers and Scanners.....	112
CHAPTER FOURTEEN	113
14. DESKTOP PC SECURITY	113
14.1 Introduction	113
14.2 Procedures	114
14.3 Commissioning and replacement:	114
14.4 Configuration.....	115
14.5 Location	116
14.6 Use.....	117
14.7 Maintenance.....	118
14.8 Disposal	118
CHAPTER FIFTEEN	119
15. ELECTRONIC RECORDS MANAGEMENT	119
15.1 Introduction	119
15.2 Roles and Responsibilities.....	119
15.3 Scope.....	120
15.4 Legal Framework.....	120
15.5 Policy Statements.....	121
15.6 Policy Principles	121
15.7 Procedures	121
15.8 Risk Assessment.....	122
15.9 Stakeholder Consultation.....	122
15.10 Documentation.....	122
15.11 Review and Monitoring.....	123
CHAPTER SIXTEEN	123
16. INCIDENT AND USER SUPPORT MANAGEMENT	123
16.1 Introduction	123
16.2 Purpose	124
16.3 Scope	124
16.4 Policy Statement	124
16.5 Types of Incidents	125
16.6 Responsibilities.....	128

CHAPTER SEVENTEEN	129
17. INFORMATION BACK UP AND RECOVERY	129
17.1 Introduction	129
17.2 Purpose	129
17.3 Scope	129
17.4 Policy Statement	129
17.5 ICT Systems/Data Backups	130
17.6 User Responsibilities	131
17.7 Data Restores	132
CHAPTER NINETEEN	133
18. WEBSITE	133
18.1 Introduction	133
18.2 Scope	133
18.3 Purpose	133
18.4 Customer Service.....	134
18.5 Content for Web Privacy Policies	134
18.6 Content Management.....	134
18.7 Privacy Policy Statements and Information Collection.....	135
18.8 Using Information.....	138
18.9 Cookies	138
18.10 Security.....	138
18.11 Changes to the Privacy Policy	139
CHAPTER NINETEEN	140
19. SOCIAL MEDIA.....	140
19.1 Introduction	140
19.2 Responsibilities of Managers.....	140
19.3 General Guidelines for the Use of SM Technologies in an Official Capacity	141
19.4 Applying for Official SM/W2.0 Accounts	145
19.5 Specific IT Security Guidelines for Using SM/W2.0 Technologies	145
CHAPTER TWENTY	147
20. EMAIL COMMUNICATION.....	147
20.1 Definition of Terms	147
20.2 Scope	147
20.3 Purpose	147
20.4 Users	147

20.5 Statement of Responsibilities	148
20.6 Guiding Principles: General Use	148
20.7 Best practices	150
20.8 Personal Use	151
20.9 Quotas and Limits.....	151
20.10 Virus Checking	152
20.11 Logging.....	152
20.12 Spam and Junk Mail	152
20.13 Remote Access	152
20.14 Incident Handling and Data Protection	153
20.15 Policy Compliance.....	153
CHAPTER TWENTY ONE.....	154
21. E-WASTE AND DISPOSAL MANAGEMENT	154
21.1 Definition of Terms	154
21.2 Operational Scope of The Policy.....	155
21.3 Fundamentals of The Policy	155
21.4 Regulatory Environment.....	155
21.5 Human Resource and Awareness	155
21.6 Effective E-waste Management Practices on Recycling	156
21.7 Sensitization on E-waste Management and Information Dissemination.....	156
21.8 E-waste Resource Mobilization.....	156
21.9 Implementation of the Policy	157
21.10 Monitoring, Evaluation and Review Strategies.....	158
CHAPTER TWENTY TWO	158
22. BYOD (BRING YOUR OWN DEVICE)	158
22.1 Definition.....	158
22.2 Purpose and Scope.....	158
22.3 Policy Statement	159
22.4 Device and Support	159
22.5 Software Allowed	159
22.6 User Obligations and County Government Disclaimers	160
22.7 Security of Systems	161
22.8 Incidents and Reporting.....	161
CHAPTER TWENTY THREE	163
23. INFORMATION SECURITY.....	163

23.1 Introduction	163
23.2 Scope	163
23.3 Responsibilities.....	164
23.4 Policy Statement.....	165
23.5 Authorised Use	166
23.6 Acceptable use.....	166
23.7 Security Awareness	166
23.8 Business Continuity.....	166
23.9 Monitoring and Reporting	166
23.10 Risk Assessment.....	167
23.11 Security Policy Review	167
23.12 Asset Management	167
23.13 Sanctions.....	167
23.14 Development of specific ICT policies, procedures and guidelines	167
CHAPTER TWENTY FOUR.....	169
SOFTWARE AND APPLICATIONS.....	169
Policy Objectives	169
Scope.....	169
Normative References	170
Software Development Policy Statements.....	170
External ICT Departments:.....	170
Project Planning & Organization.....	171
Requirements Phase.....	171
Design Phase.....	171
Monitoring and Evaluation	172
MIS Support and Use	172
Technical Support.....	172
User Requests	172
Response to Requests	172
This shall be done as per the ICT Department service charter	172
Data Collection and Updates	172
Tracing Data Update.....	172
Project Team for Each System	173
System Ownership	173
Accessibility to Information Systems.....	173

CHAPTER TWENTY FIVE	174
24. BREACHES OF POLICY	174
24.1 Network Security	174
24.2 Wireless Access	174
24.3 Access Control.....	175
24.4 Server Security	175
24.5 Public Internet Access	176
24.6 Third Party Connection	176
24.7 ICT Asset Management	177
24.8 Server Security	177
24.9 Encryption	178
LIST OF THE CONTRIBUTORS	179
REFERENCES	179

127

147

ABBREVIATIONS AND ACRONYMS

ACL:	Access Control List
APOC:	Administrative Point of Contact
BYOD:	Bring Your Own Device
CAPA:	Corrective and Preventative Action
CCTV:	Closed Circuit Television
CECM	County Executive Committee Member
CGN	County Government of Nyeri
CIO	Chief Information Officer
CO	Chief Officer
E-Waste:	Electronic Waste
ICT:	Information and Communication Technology
ID:	Identification
IS:	Information System
ISO:	International Organization for Standardization
ITS:	Integrated Telephony Systems
IDS:	Intrusion Detection Systems
IT:	Information Technology
IP:	Internet Protocol
LAN:	Local Area Network
PC:	Personal Computer
PDA:	Personal Digital Assistant
PIN:	Personal Identification Number
SM:	Social Media
TCP:	Transport Control Protocol
NC:	Nyeri County
VPN:	Virtual Private Network
CS:	County Secretary

CHAPTER ONE

1. Introduction

This Chapter contains policy statements on Information and Communication Technology (ICT) services and Information Systems that are of strategic importance to the County Government.

1.1 ICT Vision, Mission and Core Values

1.1.1 Vision

To be the preferred choice for the delivery of innovative and integrative ICT solutions and services

1.1.2 Mission

To champion and advance the development of ICT and its use by key stakeholders for the socio-economic transition and development of Nyeri County

1.1.3 Core Values

Integrity: We embrace the highest standards of ethical behavior in every aspect of our business to yield a department that is trusted by its clients and stakeholders. The transparency of our actions is consistently exemplified both internally and externally in the work we produce. We also proudly foster the values of honesty and sincerity.

Partnership: Our success and delivery of quality programmes and services are largely dependent upon the partnerships that we create with all of our internal and external stakeholders. At the Directorate of ICT, we understand that working collectively with our public and private sector stakeholders will ensure that our outputs are directly focused on satisfying the needs of all involved. We ascribe to the belief that the —whole is greater than the sum of its parts, and we promote this spirit of partnership in all that we do.

Excellence: Our commitment to professional excellence ensures that our clients receive the highest quality service. We aspire to provide flawless execution and delivery of our products and services and employ the best talent to ensure that we meet our commitments.

Teamwork: Our culture of teamwork allows us to combine the quality and expertise of our professional staff to deliver optimum solutions to our clients. We respect each other and communicate openly in an environment that fosters collaboration while still maintaining individual accountability.

Innovation: We thrive on creativity and ingenuity. In today's fast-paced technological climate, innovative ideas, concepts, and processes are essential to the continued success and growth of an organization. At the Directorate of ICT & EGovernment, we strive to create value, deliver results, and continuously improve all elements of our business. We aim to be intelligent, integrative and innovative while creating efficiency in order to provide the best solutions for clients.

Leadership: The spirit of leadership is instilled in every ICT staff. The Directorate of ICT aims to be at the forefront of the ICT revolution in order to effect positive social, economic and environmental change. We are committed to the development and execution of sound strategies and initiatives that amount to an effective display of thought leadership that will in turn solidify this county 's position on the global stage.

Communication: We ensure that we communicate openly, accurately and in a timely manner with our stakeholders: clients, employees, partners and vendors/suppliers. This is done through information-sharing and engaging in the practice of clearly explaining the expected outcomes of undertakings to all staff at all times.

Citizen Participation: We ensure that in all aspects of our business, participation by key stakeholders is mandatory. We strive for transparency and openness to promote accountability in our work.

1.2 Objectives and Strategies

- a. Support efficient acquisition of ICT resources
- b. Promote efficient use and utilization of the ICT infrastructure.
- c. Ensure Cyber Security.
- d. Improve provision of ICT services within the county government.

Objective One: To standardize acquisition of ICT Resources

Strategies:

- i. To create standardized specifications for ICT Resources.
- ii. To utilize available resources prudently.
- iii. To Standardize equipment and software resources in the County.

Objective Two: To improve ICT infrastructure.

Strategies:

- i. To develop infrastructure development plan.
- ii. To develop a repair and maintenance plan.
- iii. To Promote efficient use and utilization of ICT infrastructure

Objective Three: To Ensure Cyber Security

Strategies:

- i. To conduct information security risk assessment.
- ii. To form an information security steering committee.
- iii. To implement Government ICT Standards- Information Security Standard.

Objective Four: To Improve provision of ICT services within the county government.

Strategies:

- i. To upgrade existing network infrastructure to latest approved standards
- ii. To hire key personnel in the various technical areas of ICT to ensure continuity and efficiency.
- iii. To ensure prompt user support and introduce job ticketing system.

1.3 Rationale

Some major reasons for formulating this ICT policy are:

- a) Due to rapidly changing technologies, planning becomes increasingly important in order to avoid incompatibility and inaccessibility.
- b) To address the severe scarcity of adequately trained and experienced analysts, software engineers, systems and network managers, coupled with their long training cycles constrains ICT developments.
- c) To tackle the scarcity of financial and managerial resources.
- d) To Integrate the County Government of Nyeri ICT policy to be in-line with the National ICT Policy.

1.4 Scope

This policy applies to any user of the County Government's information and communication technology resources, whether initiated from a computer located on or off-county. This includes any computer and information system or resource, including means of access, networks, and the data residing thereon. Users are subject to both the provisions of the policy and any policies specific to the individual systems they use. Nyeri County Government ICT policy subscribes to the Kenya national ICT policy and all other policies and national legal instruments guiding the sector

1.5 Purpose

The principal concern of this policy is the effective and efficient (responsible) use of information and communication technology resources. The primary focus is to insure that the resources are used in a manner that does not impair or impede the use of these resources by others in their pursuit of the mission of the County Government.

This policy is intended to ensure that:-

- The integrity, reliability, and good performance of County ICT resources;

- The resource-user community operates according to established policies and applicable laws;
- These resources are used for their intended purposes; and
- Appropriate measures are put in place to ensure the policy is honored and adhered to.

The policy is intended to permit, rather than proscribe, reasonable resource-user access within County priorities and financial capabilities

1.6 Guiding Principles

The following principles should guide the policy's application and interpretation:

1. Freedom of thought, inquiry, and expression is a paramount value of the County Government community. To preserve that freedom, the community relies on the integrity and responsible use of County resources by each of its members.
2. The Governor is ultimately responsible for implementation of this policy, but may delegate this responsibility. The Governor shall reserve the right to determine the extent of consultation with the County Executive while implementing decisions relating to this policy.
3. Information and Communication Technology (ICT) resources are provided to support the County's mission of championing and advancing the development of ICT and its use by key stakeholders for the socio-economic transition and development of Nyeri County. To ensure that these shared and finite resources are used effectively to further the County's mission, each user has the responsibility to:
 - a. use the resources appropriately and efficiently;
 - b. respect the freedom and privacy of others;
 - c. protect the stability and security of the resources; and
 - d. understand and fully abide by established County policies and applicable public laws.
4. Responsible use of County ICT resources to advance Principle 3 above will be given priority under the prevailing or potential design, capability or functionality of specific ICT resources including operating systems, hardware, software, and the Internet.

5. Users of ICT resources are expected to uphold the highest ethical/moral standards in accordance with other applicable County policies and practices.

1.7 Policy Application

1. All existing Kenyan laws and County regulations and policies shall apply, including not only laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. This may also include laws of other countries where material is accessed electronically via County resources by users within those jurisdictions or material originating within those jurisdictions is accessed via County resources.
2. As a matter of policy, the County Government protects expression by members of its community and does not wish to become an arbiter of what may be regarded as "offensive" by some members of the community. However, in exceptional cases, the County Government may decide that such material directed at individuals or classes of individuals presents such a hostile environment under the law that certain restrictive actions shall be warranted.
3. The County Government reserves the right to limit access to its resources when policies or laws are violated and to use appropriate means to safeguard its resources, preserve network/system integrity, and ensure continued service delivery at all times.
4. References within the policy to external documents are provided solely for reference and convenience of readers. It should not be viewed as though the referenced document is being incorporated into this policy except where expressly stated or specified in the policy itself.

1.8 Laws and Regulatory Framework

This ICT Policy derives its powers from the existing laws of Kenya. The following are legal framework governing this policy:

- Constitution of Kenya 2010
- The Computer Misuse and Cybercrimes Act, 2018
- Kenya Information and Communications Act 2009;
- The National ICT Policy,
- Data protection association bill of 2009
- Access association bill of 2007
- Environmental management and co-ordination (e-waste management)

Regulations, 2013.

- The Copyright, Designs And Patents Act (1986) , and
- any other relevant legal provision and Government policies that may come into force after initial implementation of this ICT Policy.

The County Government and Third Parties shall also comply with any contractual requirements, standards and principles required to maintain the business functions of the County Government including:

- a) Protection of intellectual property rights;
- b) Protection of the authority's records;
- c) Compliance checking and audit procedures;
- d) Prevention of facilities misuse;
- e)

1.9 Policy Provisions

This section is not intended to provide a full accounting of applicable laws and policies. It is rather intended to highlight major areas of concern with respect to responsible use of County Government resources and specific issues required by law or the ICT policy.

1.9.1 Authorized Use / Access

Gaining access to the County Government's information technology resources does not imply the right to use those resources. The County Government reserves the right to limit, restrict, remove or extend access to and privileges within; material posted on, or communications via its information technology resources, consistent with this policy, applicable law or as the result of County Government disciplinary processes, and irrespective of the originating access point.

1.9.2 Data Security, Confidentiality and Privacy

County Government users are responsible for ensuring the confidentiality and appropriate use of institutional data to which they are given access, ensuring the security of the equipment where such information is held or displayed, ensuring the security of any accounts issued in their name, and abiding by related privacy rights of students and staff concerning the use and release of personal information, as required by law or existing policies.

1.9.3 Electronic Information Retention and Disclosure

Original electronic materials on central computing equipment and/or copies may be retained for specified periods of time on system backups and other locations stipulated herein; however the County Government does not warrant that such information can be retrieved.

Unless otherwise required by law and/or policy, County Government reserves the right to delete stored files and messages to preserve system integrity. Except in an emergency, users will be given ample advance notice to save any personal files and messages.

1.9.4 Network and System Integrity

In accordance with the Kenyan law, International laws and other policies, activities and behaviours that threaten the integrity of computer networks or systems are prohibited on both County Government-owned and privately-owned equipment operated on or through County Government resources.

1.9.5 Commercial Use

Use of the County Government's information technology resources for unauthorized commercial activities, personal gain (private or otherwise), unrelated to the County Government business, or fundraising is strictly prohibited.

1.9.6 Fraud

Use of County Government information technology resources for purposes of perpetrating fraud in any form is strictly prohibited.

1.9.7 Political Campaigns

The policy invokes the Kenya Government law that prohibits the use of state resources for political campaign activity.

1.9.8 Harassment

It shall be a violation of this policy to use electronic means under the County Government's jurisdiction to harass or threaten others either directly or by creating a hostile environment.

1.9.9 Copyright and Fair Use

Kenyan government law on copyright and fair use⁴ applies to all forms of information, including electronic communications, and violations are prohibited under this policy.

1.9.10 Trademarks and Patents

Unauthorized use of patents, trade secrets and trademarked names or symbols is prohibited. Use of County Government's name and symbols must comply with the County Government Intellectual Property Policy.

1.9.11 Electronic Communications

Electronic mail, news posts, chat sessions or any other form of electronic communication must comply with County Government's Privacy of Electronic Information and Communications Policy.

1.9.12 Web Sites

Both official and unofficial web sites shall be subject to the provisions of this policy, if they use County Government resources such as County Government-owned servers and the network to transmit, receive and store information.

1.10 Policy Compliance and Sustainability

The ICT is authorized by the County Executive to ensure that the appropriate processes to administer the policy are in place, communicated and followed by the County Government community and stakeholders.

1.11 Consequences of non-compliance

Enforcement shall be based upon receipt by Governors' Office Department of one or more formal complaints about a specific incident or through discovery of a possible violation in the normal course of administering information technology resources. Inappropriate use of ICT resources may result in personal, criminal, civil or other administrative liabilities.

1.12 Reporting irresponsible or inappropriate use

The CS as a designee of the County Executive shall be responsible for assessing violations to this policy and shall act in accordance with County Government policies and guidelines for investigations and resolution of problems. Policy violation cases touching on staff or members of the public shall be referred to the respective County Government disciplinary committees for deliberation or to relevant government agencies for appropriate action where necessary.

1.13 Policy review and practices oversight

The Governors' Office Department shall review this policy on an annual basis or as the need arises, make recommendations for any changes, and provide oversight and periodic review of the practices used to implement the policy.

1.14 Related requirements

ICT services and systems shall be wholesomely incorporated in the County Government's administrative and managerial processes.

CHAPTER TWO

2. NETWORK SECURITY

2.1 Introduction

The County Government of Nyeri has a large and complex ICT infrastructure. The foundation of this structure is the Data and Communications Network which is facilitated and supported by many types of hardware including extensive cabling and supporting systems installed throughout the County Government's various buildings and offices across the county.

The County Government relies heavily on its Data and Communications Network infrastructure to:

- a) Carry out its business functions and activities using connected IT systems
- b) Communicate via Integrated Telephony Systems (ITS)
- c) Facilitate Video Conferencing Technologies
- d) Provide wireless –Hot Spot access zones and ICT connected services to the public

2.1.1 Purpose

The purpose of this policy is to ensure the security, integrity and availability of the County Government's Data and Communications Network and to establish professional good working practices and procedures.

2.1.2 Scope

The scope of this policy extends to all administration, installation and configuration of the County Government's Data and Communications Network equipment and associated systems which form part of the County Government's IT infrastructure and which falls under the responsibility of the County Secretary. This policy must be undertaken in line with all existing County Government policies and procedures.

2.2 Policy Statement

The County Government's Data and Communications Network equipment is maintained and installed across most County Government buildings and locations. The County Government's main headquarters at Nyeri is the location

for the Server Room. The Server Room houses most of the Data and Communications Network equipment and serves as the main access area to the County Government's ICT Infrastructure. A second Server Room shall be established in undisclosed location (For Security Reasons) as a standby or failover location in the event that the main Server Room is inoperable.

The Chief Officer for Governors' Office shall appoint a Network Administrator who manages the data and communications network. To secure the data and communications network, the Network Administrator must ensure:

- 2.2.1** All visitors to the data and communications network environment are issued with an authorised County Government visitors badge and are signed in/out using the correct procedures (Server Room's Physical Access Control Policy).
- 2.2.2** Any visitors to the Data and Communications Network environment area must be accompanied at all times by authorised County Government personnel.
- 2.2.3** Any person not known to Network personnel must be challenged in order to establish who they are and whether authorisation has been provided for them to be there
- 2.2.4** Access to and knowledge of door lock codes are restricted to authorised personnel only and must not be shared with any unauthorised person.
- 2.2.5** Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the Server Room Manager in line with professional best practice and immediately when an employee (who has access to sensitive ICT areas) ceases to be employed by the County Government.
- 2.2.6** Electronic access tags must be issued to authorised staff on an individual basis. Staff issued with access tags must have their names and employee numbers recorded against the registered access tag number including date and time of issue.
- 2.2.7** Access tags should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorised personnel may be permitted to use another authorised person's tag if available with permission of the line manager and the recorded user must either be present or be made aware that their tag is being used. Any such use must be recorded

and maintained in a logging system for this type of event and be securely stored with restricted access.

- 2.2.8** Access to the Server Room area, including any adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms
- 2.2.9** Access tags issued to personnel who no longer work for the County Government must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system
- 2.2.10** Doors which provide access to Data and Communications Network equipment must not to be left/wedged open unless for the purpose of taking delivery of new equipment, to accommodate the movement of existing equipment, transportation of maintenance or cleaning equipment – an authorised member of staff must be present at all times to supervise access when doors are left open
- 2.2.11** All County Government cleaning staff/contracted cleaners must have and display appropriate identification and be made aware of the requirements within this policy
- 2.2.12** Personal, special access visits from relatives or acquaintances of personnel are not permitted within the secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure
- 2.2.13** Any issues to do with official authorisation of access to the Server Room area should be sought from the Server Room Manager. In the absence of the Server Room Manager, clearance should be requested from the Server Room's immediate supervisor or the Chief Officer.

Note: All staff must abide by the Server Room's Physical Access Control Policy which is available from the Server Room manager. (See Chapter Four on Access Control)

2.3 Environment

The Server Room accommodates ICT infrastructure equipment from both the Network and Server support teams. Access to the Server Rooms given by personnel from either team to visitors must be formally authorised by the Server Room Manager as any access given will be providing access to both Network and Server infrastructure equipment. In the absence of the Server Room Manager, formal clearance must be requested from the Chief Officer.

It is important to maintain a high level of professionalism to ensure the security, integrity and safety of the County Government's Data and Communications Network and supporting environment. The Server Rooms are sensitive ICT areas and as such, require a high degree of physical and environmental controls. The Server Room's **Physical Access Control** (See *Chapter Four on Access Control*) describes these controls.

All authorised personnel must ensure that they comply with the policies, procedures and best practice specific to the Data and Communications Network and Server Room working environment.

2.4 Configuration and Maintenance

Administration, maintenance and support for the County Government's ICT Network infrastructure is normally provided by a dedicated team of Network Support personnel. The following must be considered in order to protect the security, integrity and reputation of the County Government:

All Data and Communications Network hardware and software should be (or in the process of being) recorded on the County Government's approved hardware and software list. (See also Chapters on ICT Asset Management and ICT Equipment Use)

- 2.4.1** All Data and Communications Network devices must be installed and maintained according to the manufacturer's guidelines in-line with all relevant County Government policies and procedures. This will also include the relevant power supplies to Data and Communications Network devices.
- 2.4.2** All Data and Communications Network hardware and software should be purchased/obtained using approved vendors through the government's procurement laws and regulations. *(See also Chapters on ICT Asset Management and ICT Equipment Use)*
- 2.4.3** Adequate levels of staffing should be provided at all times – particularly for call-out purposes or systems requiring out-of-hours support
- 2.4.4** Firmware updates/upgrades to Data and Communications Network hardware must only be undertaken if there is an identified requirement or need to do so in line with the documented maintenance procedures.
- 2.4.5** Any visitors, contractors or vendors carrying out hardware/software installations and/or maintenance should not be left unattended while working - unless authorised by the Server Room Manager or an appropriate supervisor. Access within the building should also be limited to areas where the work is to be carried out. *(See Also Chapter on Third Party Connection)*
- 2.4.6** Data and Communications Network devices must be located in physically secure areas (locked communications rooms or cabinets) to protect against unauthorised access, removal, disconnection, interference and/or damage.
- 2.4.7** All unnecessary services running on network devices must be disabled wherever possible
- 2.4.8** Controls must be implemented to prevent direct unauthorised communication with network devices (Infrastructure ACLs).
- 2.4.9** Logical separation of the network must be implemented at Layer 2 Virtual Local Area Networks (VLANs) and layer 3 (subnets) with access controls implemented (Private VLANs, Access Control Lists (ACLs), firewalls).
- 2.4.10** All routing protocol exchanges must be authorised and verified.
- 2.4.11** All security devices deployed must be EAL4 compliant

- 2.4.12** Data cables should be individually identifiable through the application of a labelling scheme to ensure cables are not removed or re-patched in error
- 2.4.13** Standardised cable colours should be used where practical to differentiate between cables carrying data and cables carrying partner data or external (service provider) connections
- 2.4.14** Configuration details and any other potentially sensitive information relating to network management must not be circulated to any party outside the Network Support team.
- 2.4.15** Disaster recovery procedures must be in place in the event of loss of the County Government's Data and Communications Network infrastructure and procedural documentation must be regularly updated to include any changes/updates to existing procedures or processes involved (*See also Chapter on Backup and Disaster Recovery*)
- 2.4.16** Data and Communications Network Infrastructure Fault Tolerance and Redundancy procedures must be in place and tested for effectiveness on a regular basis. Procedural documentation must be regularly updated to include any changes or updates
- 2.4.17** Network Management procedures must be in place for the administration of all critical network functions including firewall maintenance, Intrusion Detection Systems (IDS), management and maintenance of Internet activity logs.
- 2.4.18** Any new hardware or systems to be installed as part of the County Government's Data and Communications Network must be provided with documentation detailing running environment specification, installation procedures and details of any known issues which could adversely affect the security and integrity of the County Government's ICT infrastructure – these requirements must be formally identified and included in system documentation and service agreements on procurement of the hardware or system
- 2.4.19** Configuration changes to the Data and Communications Network must be passed through the County Government's Directorate of ICT. Procedures and any planned work to be scheduled should include a notification to all parties affected via the same office.
- 2.4.20** Emergency Changes will follow the agreed Emergency Change Procedure which requires emergency changes to be approved by

designated staff and for the changes to be documented and submitted retrospectively

2.4.21 In the event of inappropriate activity or network misuse being identified by the Network Team this should be reported immediately via the Security Incident Reporting mechanism and where there is suspected fraud or serious system misuse reported to all relevant investigative organs of the County Government.

2.5 Administration

2.5.1 Administrative access for the management of Data and Communications Network devices is permitted only from authorised management workstations defined by the Network Support team

2.5.2 Authorised personnel with administrative access to Data and Communications Network devices and/or Servers must have their account disabled immediately on suspension from or cessation of employment with the County Government.

2.5.3 Administrative access for the management of network devices is permitted only for authorised personnel. All administrative management access must be monitored (including failed access attempts) and event logs must be checked for events such as unauthorised access attempts

2.5.4 Only authorised personnel are provided with full administrative access to network infrastructure devices – read-only access may be made available to other parties where necessary. *(See also Chapters on Access Control)*

2.5.5 All interfaces used for system administrative management must be appropriately secured

2.5.6 All administrative/management sessions and data must be protected through the use of secured protocols in accordance with industry best practice. *(See also Chapters Data Protection and Information Systems)*

2.5.7 All passwords in the network device configuration must be encrypted. *(See also Chapters on Encryption and Password Management)*

2.5.8 Local device passwords must be changed quarterly and must conform to the County Government's Password Policy wherever possible. *(See also Chapters on Encryption and Password Management)*

- 2.5.9** Password recovery must be disabled on all devices - backup configurations must be readily available in case of emergency. *(See also Chapters on Encryption, Password Management and Backup & Disaster Recovery)*
- 2.5.10** Copies of backup passwords must be kept in secure locations both onsite and offsite and easily accessible to authorised staff when required. *(See also Chapters on Encryption, Password Management and Backup & Disaster Recovery)*
- 2.5.11** Notifications which display acceptable (authorised) use including warnings for unauthorised use must be presented to any user connecting to infrastructure network devices. *(See also Chapters on Access Control)*
- 2.5.12** All Data and Communications Network equipment which may require local logon privileges for configuration and maintenance i.e. Routers etc... must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of the County Government's Password policy wherever possible. *(See also Chapters on Encryption and Password Management)*
- 2.5.13** All administrative, privileged systems account passwords (not individual user accounts) must be stored using encryption which utilizes a minimum of 128 Bit AES encryption and must only be accessible to Network Support personnel. *(See also Chapters on Encryption and Password Management)*

2.6 Monitoring and Event Logging

- 2.6.1** Network events which include the following must be logged and recorded to a centrally secured location:
- a) Security events
 - b) Network device access
 - c) Systems warnings errors or critical alerts
 - d) CPU and memory threshold alerts
 - e) Routing change events
 - f) Network topology changes
 - g) Servers which are used to log events/data files must be appropriately secured against unauthorised access in line with the County

Government's Server Security procedures. (See also Chapters Procedures on Network Security and Server Room Management)

- 2.6.2** Logging events to individual network devices must be disabled
- 2.6.3** Log files must be routinely analysed to ensure anomalies, failures, unexpected changes or any other significant events are reported under the County Government's incident/event management process.
- 2.6.4** All network device clocks must be synchronised with a central time.
- 2.6.5** Network traffic profiles must be monitored and analysed for capacity management and anomaly detection.

2.7 Remote Access

- 2.7.1** Procedures must be in place to ensure that any external remote connections enabled for third party software/system support to the County Government's Network/Servers are setup in accordance with the

County Government's IT Security Policies and connect via the County Government's VPN portal. *(See Also Chapter on Third Party Connection)*

- 2.7.2** The Network Support team must ensure that the correct procedures and processes are in place to facilitate and enable third party vendors to provide support for the County Government's software and systems using

the most secure methods available. *(See Also Chapter on Third Party Connection)*

- 2.7.3** Access accounts used to provide third party support are only enabled when required and disabled immediately when not required including regular account password changes. Documentation detailing this process must be developed and disseminated to relevant areas such as the ICT Service Desk in order to protect the County Government's Network and Server infrastructure. *(See Also Chapter on Third Party Connection)*

- 2.7.4** The Network Support team should facilitate County Government staff accessing the County Government Network/Servers remotely and the team should ensure users are restricted to using the most secure protocols and tunnelling mechanisms available. *(See Also Chapters on Third Party Connection)*

2.7.5 Network Support staff working remotely or from home must observe the same controls and procedures as when working within the County Government offices in order to ensure the security, integrity and to prevent loss and/or damage to the government assets and reputation. *(See Also Chapter on Third Party Connection and Acceptable Use)*

CHAPTER THREE

3. WIRELESS SECURITY

3.1 Introduction

Wireless Local Area Networks (LANs) form part of the County Government of Nyeri's corporate network infrastructure. In order to protect the business needs of the government the wireless, network must meet the same level of security employed by the rest of the infrastructure.

This policy is to ensure that the deployment of wireless networking is controlled and managed in a centralised way to provide functionality and optimum levels of service whilst maintaining network security.

The intention of this policy is to define roles and responsibilities for the design of any emerging wireless network, the installation, registration and management of wireless access points and devices, adequate management allocation of the wireless frequency spectrum and the services offered to end users for wireless access.

3.2 Purpose

This policy outlines a common set of procedures and operational criteria for the effective management of 802.11 wireless LANs. Due to the characteristics of Wireless technology, all wireless developments must be planned, deployed and managed in a carefully controlled manner, and developed in accordance with the County Government's Information Security Policy.

The three main areas that the wireless policy will address include:

3.2.1 Security

Wireless LANs offer connectivity to anyone within range of an Access Point; physical boundaries are no longer a relevant option for preventing access to the network. Installations of non-approved devices which may be configured with little or no security increase the risk of a breach of security of the County Government's data network and are prohibited.

3.2.2 Non-Standard Devices

Non-standard or misconfigured wireless devices can cause disruptions to the wireless LANs and subsequently the wired network. The County Government therefore prohibits the installation of any non-standard wireless access points.

Only wireless network equipment authorised and installed by the ICT Department is permitted on the County Government's network.

3.2.3 Interference

Wireless technology compliant with the 802.11 standards uses frequencies from a band which is divided into channels. In order for adjacent access points to work with each other and not cause interference or performance issues, a different channel must be used for each Access Point.

3.3 Policy Statement

The County Government's Wireless Network and equipment is maintained and installed across most of its buildings and locations and becomes part of its Communication Network for the County Government.

3.4 Scope

3.4.1 This Chapter of the ICT policy applies to all areas of wireless connectivity to the County Government's network infrastructure, and includes all wireless devices operating within the County Government's IP address range, on any of the County Government's premises, or any remote location directly connected to the County Government's data network. The policy describes the standards that users are expected to observe when using the County Government's wireless facilities and details the potential consequences for misuse.

3.4.2 The Directorate of ICT is responsible for the County Government's network infrastructure. The wireless network is an extension to this network and therefore the department has the responsibility for the design, deployment and management of the County Government's wireless LANs.

3.5 Restrictions

3.5.1 All Access Points and wireless devices used by staff on the County Government's secure wireless network must conform to all related national regulations, standards and recommended specifications as defined by The Directorate of ICT

3.5.2 All new Access Points and wireless devices used by staff on the County Government's secure wireless network must be purchased and installed by the Directorate of ICT, in-line with the government's current purchasing policy and IT Standards.

3.5.3 All Access Points and wireless devices used by staff on the County Government's secure wireless network must follow The Directorate of ICT standard configuration settings.

- 3.5.4** The installation of any non-standard Access Points or wireless devices is prohibited.
- 3.5.5** The Directorate of ICT has the right to disable any nonstandard, unauthorised devices which may cause interference with existing approved Access Points or devices. Such devices may be removed without prior notice.
- 3.5.6** Monitoring of wireless networks is undertaken by The Directorate of ICT on a regular basis.
- 3.5.7** Wireless security testing will be performed on a periodic and random basis using audit penetration tests involving skills and tools commissioned from independent third party companies. However, all penetration tests carried out internally must have prior approval from the officer responsible for networks and the Chief Officer responsible for Governors' Office. The use of unauthorised wireless security testing on the County Government's network is considered a disciplinary matter up to and including gross misconduct.
- 3.5.8** New requests for the installation of new Access Points or wireless devices must be directed through the Chief Officer responsible for Governors' Office.
- 3.5.9** Unauthenticated open access to the Internet may be provided separately from the secure wireless network via wireless hot spots in the County Government's public buildings. Access via personal laptops and other mobile devices will be subject to internet filtering.

3.6 Appropriate Use

- 3.6.1** The County Government supports the appropriate and proper use of services and facilities that it provides to staff and other authorised users. Only Nyeri County Government approved software and hardware devices are permitted on the County Government's secure wireless network. *(See Also Chapter on Third Party Connection and Acceptable Use)*
- 3.6.2** Failure of Contractors, Agency Staff, Partners/Agencies or Third Party Organisations to comply with this policy may result in termination of contracts and connections, suspension of services and where appropriate, in accordance with the terms of individual contracts and agreements, the County Government may also seek to recover any loss incurred as a result. Where the County Government considers it appropriate, inappropriate use of the County Government's wireless facilities will be reported to the relevant government agencies.

3.6.3 Failure of employees to comply with this policy may result in disciplinary action being taken against them.

3.7 Regulatory Framework

3.7.1 The County Government of Nyeri takes responsibility for providing an appropriate regulatory framework, including specific standards and guidance relating to the appropriate use of these County Government services and facilities. The Wireless Network Policy constitutes a component part of this framework.

3.7.2 Business use of all ICT facilities provided by the County Government is subject to the relevant Policies and Regulations, in particular the County Government's Internet and e-mail policy, Safe Haven, Information Security policy and Acceptable Use policy.

3.8 Acceptance

3.8.1 All users of information and ICT systems for which the County Government is responsible must agree to, and abide by, the terms of County Government of Nyeri's Acceptable Use part of the ICT Policy *(See Also Chapter on Third Party Connection and Acceptable Use)* associated security policies and applicable Codes of Conduct.

3.9 Roles and Responsibilities

All Wireless LANs are monitored and maintained by the Directorate of ICT. Any Access Point or wireless device which is connected to the County Government network infrastructure becomes the responsibility of the Directorate of ICT .

3.10 User responsibilities

3.10.1 Users of the County Government's secure wireless network must not connect any unauthorised equipment to the County Government data network without prior approval from the Chief Officer responsible for ICT or an authorised officer appointed by the Chief Officer. If The Directorate of ICT deems that any particular equipment may be the cause of unacceptable degradation of the performance of the network or poses a security risk, then the user must cooperate with the disconnection of that equipment from the network. *(See Also Chapter on Third Party Connection and Acceptable Use)*

3.10.2 Wireless technology must not be used to connect to secure systems such as financial management information systems. Connection to these systems should be made using a designated County Government provided PC utilising the County Government's —wired network only. Home working solutions for connection to County Government's financial management information systems are not permitted at this stage; however, this may be reviewed and communicated appropriately at a later stage. *(See Also Chapter on Third Party Connection and Acceptable Use)*

3.10.3 All users accessing authorised wireless equipment must abide by the County Government's Acceptable Use Chapter of the ICT Policy, associated security policies and applicable Codes of Conduct. *(See Also Chapter on Third Party Connection and Acceptable Use)*

3.10.4 Apart from notification of the availability of the guest —Open wireless network, no information regarding the wireless network, including configuration and setup information, should be shared with any unauthorised users, third party vendors or members of the public. *(See Also Chapter on Third Party Connection and Acceptable Use)*

CHAPTER FOUR

4. ACCESS CONTROL

4.1 Introduction

Availability, confidentiality and integrity are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital for the protection of systems and information that authorised users who have access to County Government systems and information are aware of and understand how their actions may affect security.

4.1.1 Availability

Systems and information are physically secure and will be accessible to authorised persons when required.

4.1.2 Confidentiality

Systems and information will only be accessible to authorised persons.

4.1.3 Integrity

The accuracy and completeness of Systems and Information are safeguarded.

4.2 Authorised Users

All parties (either as part of a contract of employment or Third Party contract) who have access to, or use of ICT systems and information belonging to, or under the control of the County Government of Nyeri including:

4.2.1 County Government employees

4.2.2 Students on attachment or internship

4.2.3 Contractors

4.2.4 Temporary staff

4.2.5 Agency staff

4.2.6 Partner organisations

4.2.7 Members of the public

4.2.8 Any other party utilising County Government of Nyeri ICT resources

4.3 Purpose

The purpose of this Chapter of the ICT Policy is to ensure that both Logical and Physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

4.4 Scope

The scope of this policy includes all access to County Government of Nyeri information, ICT systems and physical access to areas and locations where information and data is located. This policy applies throughout the information lifecycle from acquisition/creation, through to utilisation, storage and disposal.

4.5 Systems and Information Access

A form exists on the County Government's intranet (NyeriNet) system for managers to complete if an employee's role within the organisation changes and access to systems needs to be updated or removed. Managers must contact the ICT Service Desk to ensure access to other systems and programs are updated if a user's role or business needs changes. The following determines System and Information Access:

- 4.5.1** For systems containing restricted and personal information and data, an access control matrix must be developed to record role-based authorised access recorded on an individual basis. Authorisation procedures must be in place for managers to authorise all access (including short term and temporary access) recorded on the matrix. The access matrix must be continually updated and maintained to reflect accurate records of access. (See Also Chapter on Data Protection and Acceptable Use)
- 4.5.2** To gain access to specific systems and information, a member of staff will need to follow a formal application process. Users will need to apply to the relevant owners/senior custodian of the systems using the appropriate completed forms.
- 4.5.3** Generic logons are not generally permitted across the County Government, however, use of generic accounts under exceptional controlled' circumstances such as the County Government's resources , is permitted.
- 4.5.4** To ensure relevant County Government or national legislation security standards are adhered to, personnel checks may be undertaken if required.
- 4.5.5** The appropriate level of access to systems and information will be determined upon the prospective users required business need, job function and role.

- 4.5.6** A signed confirmation by the user may be required indicating that they understand and appreciate the conditions of access and security.
- 4.5.7** If authorisation to use systems and information is granted, unique logon credentials and password will be provided to the applicant. Further instruction on how to maintain the security of systems and information with due regard to the procedures below may be given. (See Also Chapter on Password Management and Acceptable Use)
- 4.5.8** Access for remote users shall be subject to authorisation by line managers via the Directorate of ICT . No uncontrolled external access shall be permitted to any network device or networked system. (See Also Chapter on Third Party Connection and Acceptable Use)
- 4.5.9** The application and all other documentation should be maintained in line with the ICT Guidelines and Standards

4.6 Systems and Information De-Registration

- 4.6.1** If a member of staff changes role or their contract is terminated, their manager should apply to have the users access to the system/information reviewed or removed as soon as possible. (See Also Chapter on Third Party Connection and Acceptable Use)
- 4.6.2** If a member of staff is deemed to have contravened any Sections of the ICT policy or procedures, potentially jeopardising the availability, confidentiality or integrity of any systems or information, their access rights to the system/information should be reviewed by the system owners. (See Also Chapter on Third Party Connection and Acceptable Use)
- 4.6.3** If a specific access limit is exceeded or control circumvented several times by a user the System Administrator should review the access rights of the user and if necessary remind the user of the relevant access and security. (See Also Chapter on Third Party Connection and Acceptable Use)
- 4.6.4** If a number of unsuccessful log-on attempts is exceeded, the user will be informed that they need to contact the system administrator or the ICT service desk to ask for access rights to be re-established. In these circumstances, access rights may need to be reviewed. (See Also Chapter on Third Party Connection, Password Management and Acceptable Use)
- 4.6.5** If it is deemed that it is no longer appropriate or necessary for a user to have access to systems and/or information then the user's manager will need to inform the owners of the system/information that access rights should be altered/removed immediately. (See Also Chapter on Third Party Connection, Password Management and Acceptable Use)

4.6.6 If any system/information rights are altered or removed, the relevant documentation will need to be updated accordingly. (Refer to Procedures and Guidelines on Information Systems)

4.7 Log-On Considerations

- 4.7.1** All systems should be accessed by secure authentication of user validation. As a minimum this should entail use of a User name and a Password.
- 4.7.2** Logon to systems/information should only be attempted using authorised and correctly configured equipment in accordance with County Government policies.
- 4.7.3** After successful logon users should ensure that equipment is not left unattended and active sessions are terminated or locked as necessary. Systems should be logged off, closed down or terminated as soon as possible.
- 4.7.4** System logon data should not be copied, shared or written down.
- 4.7.5** Note: (See Also Chapter on Third Party Connection, Password Management and Acceptable Use)

4.8 Physical Access and Controls

Maintaining the physical security of offices and rooms where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information and data:

- 4.8.1** Staff should wear their officially provided County Government identification (ID) badges and visitors must wear the Visitor ID badges. People who are not displaying ID badges should be prohibited from accessing those restricted areas. Any person not known to location personnel must be challenged in order to establish who they are and whether authorisation has been granted for them to be there. If there is any doubt about the identity of the individual, the appropriate security officer/manager should be contacted to confirm the individual's identity.
- 4.8.2** Appropriate recording mechanisms need to be in place to record the names, dates, times and signatures for the signing in and out of visitors (including County Government personnel) to County Government locations and critical establishments. All visitors must be issued with an authorised County Government visitors badge when signing in.
- 4.8.3** The use of keys to buildings, rooms, secure cabinets, safes etc. must be controlled and recorded. Keys must be stored in secure areas/locked

cabinets when not in use and must be identifiable by recording serial/ID markings of all keys. The location of keys must be known at all times and a signing in/out recording mechanism must be maintained to record the serial/ID of keys against individual names when keys are used.

- 4.8.4** Electronic access fobs (Definition: small security hardware device with built-in authentication used to control and secure access to network services) must be issued to authorised staff on an individual basis. Staff issued with access fobs must have their names and employee numbers recorded against the registered access fob number including date and time of issue
- 4.8.5** Access fobs should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorised personnel may be permitted to use another authorised person's fob if available with permission of the line manager and the recorded user must either be present or be made aware that their fob is being used. Any such use must be recorded and maintained in a logging system for this type of event
- 4.8.6** Access fobs issued to personnel who no longer work for the County Government of Nyeri must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system
- 4.8.7** Locations housing critical or sensitive information and/or information processing facilities should have a secure, physically sound perimeter with suitable controls and restrictions allowing access to authorised staff

only. CCTV and audible alarm systems should be active in areas where critical servers are located, such as in the Server Room.
- 4.8.8** Observance and maintenance of the physical security of rooms and offices where PCs and/or critical information processing equipment is located needs to be a paramount consideration. For example, do not house critical equipment in publicly accessible locations, close to windows, in areas where theft is a high risk. Locate servers and business critical equipment in locations with adequate environmental and fire controls.
- 4.8.9** Access to information processing systems will only be allocated to staff following any required legal/County Government checks. If required, usage policies will also need to be signed by staff.
- 4.8.10** All interfaces used for managing system administration and enabling access to information processing must be appropriately secured.
- 4.8.11** Access to and knowledge of key fobs, door lock codes or access to keys for locks, are restricted to authorised personnel only and must not be shared with any unauthorised person.

- 4.8.12** Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the location manager in line with professional best practice.
- 4.8.13** If electronic door locks/key fobs are in use they must be issued to authorised staff on an individual basis, be fully registered to that individual and only used by that individual. The key fob must be deactivated immediately when no longer required and registration details updated accordingly.
- 4.8.14** If biometric access is required to access certain areas, it must be provided to specified persons whose details are properly captured and should be used for only the provided purpose.
- 4.8.15** Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms.
- 4.8.16** All County Government/Contracted Cleaners must have and display appropriate identification and be made aware of the requirements within this procedure.
- 4.8.17** Personal, special access visits from relatives or acquaintances of personnel are not permitted within secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure.
- 4.8.18** Trips – prior arrangements should be made and authorised before visiting sensitive installations such as the Server Room
- 4.8.19** Equipment should be sited to minimise unnecessary, unauthorised access into work areas. For example, refreshment units or office machinery designed for visitors should be placed in public accessible areas only.

4.9 Responsibilities

- 4.9.1** Chief Officers of respective departments are responsible for ensuring that all staff and managers are aware of security policies and that they are observed.
- 4.9.2** Managers need to be aware they have a responsibility to ensure staff hold sufficient, relevant knowledge concerning the security of information and systems.
- 4.9.3** Designated owners of systems, who have responsibility for the management of ICT systems and inherent information, need to ensure that staff have been made aware of their responsibilities toward security.
- 4.9.4** Designated owners of systems and information need to ensure they uphold the security policies and procedures.

CHAPTER FIVE

5. SERVER ROOM & SERVER SECURITY

5.1 Introduction

The County Government of Nyeri has a large and complex ICT infrastructure. Servers form a key part of this infrastructure - providing essential services, access to computer applications, security and data storage. The County Government's ICT network would be unable to function or provide its critical services without the availability of servers.

All administration, installation and configuration of servers and associated systems which form part of the County Government's IT infrastructure and which fall under the responsibility of the Server Room Support team must be undertaken in line with all existing County Government policies and procedures.

5.2 Purpose

The following details the security implications and measures required to ensure the County Government's Server infrastructure is protected through effective and well managed procedures and practices.

5.3 Scope

This policy applies to all County Government servers which are maintained and installed within secure County Government buildings and locations. The County Government's main headquarters at Nyeri is the location for the Server Room. The Server Room houses most of the Server and Network equipment and serves as the main access area to the County Government's ICT Infrastructure. A second Server Room will be established at undisclosed location as a standby or failover location in the event that the main Server Room is inoperable.

5.4 Policy Statement

The County Government shall appoint a Server Room Manager who manages the Server Room and Server Infrastructure to ensure maximum efficiency and effectiveness at all times and thus ensure security of critical systems and data.

5.5 Server Room Security

To secure the Server Rooms the Server Room Manager must ensure that:

- 5.5.1** Appropriate mechanisms are in place to record the names, dates, times and signatures for the signing in and out of visitors (including County Government personnel) to the Server Room. All visitors must be issued with an authorised County Government visitors badge when signing in
- 5.5.2** Any visitors to the Server Room area must be accompanied at all times by authorised County Government personnel
- 5.5.3** Any person not known to Server Room personnel must be challenged in order to establish who they are and whether authorisation has been provided for them to be there
- 5.5.4** Access to and knowledge of door lock codes are restricted to authorised personnel only and must not be shared with any unauthorised person.
- 5.5.5** Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the Server Room Manager in line with professional best practice and immediately when an employee (who has access to sensitive ICT areas) is transferred or ceases to be employed by the County Government
- 5.5.6** Electronic access tags must be issued to authorised staff on an individual basis. Staff issued with access tags must have their names and employee numbers recorded against the registered access tag number including date and time of issue
- 5.5.7** Access tags should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorised personnel may be permitted to use another authorised person's tag if available with permission of the line manager and the recorded user must either be present or be made aware that their tag is being used. Any such use must be recorded and maintained in a logging system for this type of event
- 5.5.8** Access to server rooms including any adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms
- 5.5.9** Access tags issued to personnel who no longer work for the County Government must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system
- 5.5.10** Doors which provide access to the servers/rooms are not to be left/wedged open unless for the purpose of taking delivery of new equipment, to accommodate the movement of existing equipment, transportation of maintenance or cleaning equipment – an authorised member of staff must be present at all times to supervise access when doors are left open

- 5.5.11** All County Government/Contracted Cleaners must have and display appropriate identification and be made aware of the requirements within this policy
- 5.5.12** Personal, special access visits from relatives or acquaintances of personnel are not permitted to secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure
- 5.5.13** Any issues to do with official authorisation of access to the Server Room Area should be sought from the Server Room Manager – in the absence of the Server Room Manager, clearance should be requested from the Chief Officer responsible for Governors' Office.
- 5.5.14** (See Also Chapter on Network Security, Access Control and Acceptable Use)

All staff must abide by the Server Room's Physical Access Control Procedure which is made available to Server Room personnel and can be requested from the Server Room manager

5.6 Environment

- 5.6.1** Servers are physically Stored/Located in the Server Room areas. The Server Room accommodates ICT infrastructure equipment from both the Server and Network support teams.
- 5.6.2** Access to the Server Rooms given by personnel from either team to visitors must be formally authorised by the Server Room Manager as any access given will be providing access to both Server and Network infrastructure equipment. In the absence of the Server Room Manager, formal clearance must be requested from the Chief Officer responsible for Governors' Office.
- 5.6.3** The Server Rooms are sensitive ICT areas and as such, require a high degree of physical and environmental controls. Some of the controls include temperature, clean environment and secure physical doors. The Server Room's Physical Access Control Procedure describes these controls.
- 5.6.4** All authorised personnel must ensure that they comply with the policies, procedures and best practices specific to the Server Room working environment.

5.7 Server Configuration and Maintenance

The County Government's Network Domain IT Infrastructure is built on and around the Microsoft Windows environment. All Servers which include critical infrastructure functions (excluding any alternative/legacy servers running disparate operating systems), are installed with Microsoft Windows Server based

operating systems (*However, other Operating Systems will be considered from time to time depending on the needs*). Administration of these Windows based Servers is normally provided by a dedicated team of Server Support personnel.

Administration, maintenance and configuration of these servers require the following considerations in order to protect the security, integrity and reputation of the County Government:

- 5.7.1** All Server hardware and software should be (or in the process of being) recorded on the County Government's approved hardware and software list. (See Also Chapter on ICT Asset Management and ICT Equipment Use)
- 5.7.2** All Server hardware and software should be purchased/obtained using approved vendors through the Government's procurement procedures and regulations.
- 5.7.3** Adequate levels of staffing should be provided at all times – particularly for call-out purposes or systems requiring out-of-hours support
- 5.7.4** All visitors, contractors or vendors carrying out hardware/software installations and/or maintenance should not be left unattended while working - unless authorised by the Server Room Manager or an appropriate supervisor. Access within the building should also be limited to areas where the work is to be carried out. (See Also Chapter Third Party Connection and ICT Acceptable Use)
- 5.7.5** Servers must be regularly updated with the latest Operating System security updates and patches. (See ICT Guidelines and Procedures on Windows Updates)
- 5.7.6** Servers must be protected from malicious software and viruses using industry standard antivirus and anti-malware software regularly updated with the latest definition and signature files whenever they become available. (See Also Chapter on Incident and Operational Management Use)
- 5.7.7** All Servers must record all logon, system and application activity via Windows event logs which must be archived off and stored securely elsewhere on a regular basis.
- 5.7.8** All unnecessary Services, Applications, and Network Protocols should be removed or disabled
- 5.7.9** All unneeded or unnecessary Default Windows Accounts should be disabled.
- 5.7.10** Backup and restore procedures and routines must be employed so that systems and data files can be restored and recovered in the

quickest, most efficient time possible. (See Also Chapter on Backup and Recovery)

- 5.7.11** Disaster recovery procedures must be in place in the event of loss of Server(s) or IT infrastructure and procedural documentation must be regularly updated to include any changes/updates to existing procedures or processes involved. (See Also Chapter on Backup and Recovery)
- 5.7.12** Server/Domain Fault tolerance and Redundancy procedures should be in place and tested for effectiveness on a regular basis and procedural documentation must be regularly updated to include any changes or updates. (See ICT Guidelines and Procedures on Windows Updates)
- 5.7.13** Any new software or systems to be installed on the County Government's Servers must be provided with documentation detailing running environment specification, installation procedures and details of any known issues which could adversely affect the security and integrity of the County Government's Server infrastructure – these requirements must be formally identified and included in system documentation and service agreements on procurement of the software/system. (See ICT Guidelines and Procedures on Information Systems Development & Acquisition)
- 5.7.14** Configuration changes to software, servers and systems must be passed through the County Government's Change Advisory Board (CAB) and any planned work to be scheduled should include a notification to all parties affected via the Change Control Procedure
- 5.7.15** Emergency Changes will be reported to the CAB during working hours where appropriate. In out-of-hours emergency situations the the Server Room Manager will use his/her professional judgement to decide on the appropriate course of action.

Back-up, Restore and Disaster Recovery procedures are in place and are available from the Server Room manager. (See ICT Guidelines and Procedures on Back-up, Restore and Disaster Recovery)

5.8 Administrative Accounts

These accounts are held by the Network Administrator, Database Administrator and Server Room Manager that provides access to the Server Room and servers. The following must be taken into consideration in managing these accounts:

- 5.8.1** All Server support staff who are provided with Domain Administrator privileges must ensure at all times that individual passwords are not

shared with anyone else – in line with the County Government's Password policy

- 5.8.2** Authorised personnel with Domain/Administrative access to servers and ICT devices must have their account disabled immediately on cessation of employment with the County Government.
- 5.8.3** Authorised personnel with administrative access to servers for maintenance, installation or configuration must logon with individual usernames and passwords wherever possible.
- 5.8.4** All Server support staff who are provided with Domain Administrator privileges must ensure their own account passwords are set to expire on a regular basis in line with existing account expiration policies and professional best practice.
- 5.8.5** All accounts (other than individual user accounts) which are used solely for the installation, maintenance and configuration of Servers, software and/or other supporting hardware equipment must be disabled prior to and after use – i.e. account only to be enabled when required
- 5.8.6** Groups and accounts added to local Server administrator or other privileged groups must be removed unless absolutely necessary – a record of Groups and accounts which are added to local Server Administrative/ privileged groups must be maintained
- 5.8.7** All ICT devices which may require local logon privileges for configuration and maintenance must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of the County Government's Password policy wherever possible
- 5.8.8** All Server administrative, privileged, software systems account passwords (not individual user accounts) must be stored using encryption which utilises a minimum of 128 Bit AES encryption and must only be accessible to Server support personnel

(See Chapter on Network Security, Encryption, Access Control and Password Management)

5.9 Service Accounts

Service accounts can be described as any account that does not correspond to an actual person. These are often built-in accounts that services use to access resources they need to perform their activities. However, some services require actual user accounts to perform certain functions.

The following considerations must be taken into account when working with service accounts and system services:

- 5.9.1** All services must be run using local/system accounts wherever possible
- 5.9.2** New software and systems procured must fulfil the requirement of using local/system accounts to run services wherever possible
- 5.9.3** All Domain accounts currently used to run services must have a password length and complexity in line with the County Government's password policy and professional best practice
- 5.9.4** Domain accounts which were configured to run a service/s but which are no longer required must be disabled and/or removed (deleted)

(See Chapter on Network Security, Encryption, Access Control and Password Management)

5.10 Remote Access

- 5.10.1** Procedures must be in place to ensure that any external remote connections enabled for third party software/system support to the County Government's Network/Servers are setup to connect via the County Government's (VPN) portal and any access via the old VPN service is disabled
- 5.10.2** The Server Support team must ensure that the correct procedures and processes are in place to facilitate and enable third party vendors to provide support for the County Government's software and systems using the most secure methods available
- 5.10.3** Access accounts used to provide third party support are only to be enabled when required and disabled immediately when not required including regular account password changes. Documentation detailing this process must be developed and disseminated to relevant areas such as The Directorate of ICT Service Desk in order to protect the County Government's Servers and network infrastructure
- 5.10.4** The Server Support team should facilitate County Government staff accessing the County Government Network/Servers remotely and should be restricted to using the most secure protocols and tunnelling mechanisms available
- 5.10.5** Server Support staff working remotely or from home must observe the same controls and procedures as when working within the County Government premises in order to ensure security and integrity and to prevent loss and/or damage to County Government assets and reputation

(See Also Chapter on Third Party Connection, Password Management and ICT Acceptable Use)

CHAPTER SIX

6. PUBLIC INTERNET ACCESS

6.1 Introduction

As part of its public service duties, the County Government of Nyeri shall provide free public access to the Internet for informational, educational and leisure needs. Sites where such facilities shall be provided are libraries, county learning establishments, guest wireless access points at designated locations, streets and recreational parks. . When providing the public internet access facility, the County Government of Nyeri recognises its obligation to protect public and County Government information, equipment and systems from threats posed via the internet, malicious conduct and accidental occurrences.

This policy details the reasoning for vigilance and the required necessary standards/guidelines with regard to security, when enabling and using public internet access.

6.2 Purpose

The purpose of this policy is to establish a set of standards and guidelines relating to public internet access. This will ensure that systems, data and equipment of both the County Government and the public remain as secure as possible. When using publicly available internet access, all County Government employees, contractors, vendors and members of the public should adhere to the policy. The aim being to ensure damage to County Government and public systems, data and equipment does not occur and prevent further damage to reputations and public services.

Guest wireless access points enabling internet access cannot be easily controlled or audited but notice of County Government's expectations regarding conduct and safety should be made available.

6.3 Scope

The scope of this policy includes:-

6.3.1 ICT equipment and systems belonging to, or under the control of County Government of Nyeri

6.3.2 Information in use on County Government ICT equipment, networks and systems.

- 6.3.3** ICT equipment and systems belonging to members of the public using public internet facilities.
- 6.3.4** Information in use on members of the public's equipment, networks and systems.
- 6.3.5** The rules, regulations, software and hardware controls incorporated into the provision of public internet access.
- 6.3.6** Internet content viewed, copied or circulated by all parties utilising County Government of Nyeri provided public internet access.
- 6.3.7** All parties who use public internet access or parties who enable public internet access, include but not limited to:
 - a) County Government employees
 - b) Students on internship or attachment
 - c) Contractors
 - d) Temporary staff
 - e) Partner organisations
 - f) Members of the public
 - g) Volunteers

6.4 Responsibilities

In the process of availing internet to all users (both internal and external as defined), County Government, Employees and Members of the public will have some responsibilities defined including but not limited to the following:

- 6.4.1** The County Government of Nyeri will provide ICT equipment and software with the correct security provisions either as a publicly available PC or as a _hotspot'.
- 6.4.2** Members of staff are responsible for ensuring that equipment is used by the public in accordance with the County Government's ICT Policy on Acceptable Use and Public Internet Access Code of Conduct (below), therefore enabling internet access but not incurring security risks.
- 6.4.3** Members of staff using County Government provided equipment for internet use are required to adhere to the associated County Government's ICT Acceptable Use policy and Public Internet Access Code of Conduct.
- 6.4.4** Members of the public, staff, residents who utilise _Guest' wireless access points or specially provisioned networked access points whilst using their own ICT equipment should be made aware of the Public Internet Access Code of Conduct and be aware that any damage to

privately owned ICT equipment resulting from incorrect usage is their responsibility.

- 6.4.5** The County Government cannot be held responsible for any financial loss or damage incurred as a result of Internet activity

6.5 Policy statement

With the continuing emphasis on provision of a public service that encompasses greater access to the internet, it necessarily becomes important to guarantee the equipment, systems and software are safe, robust and the ongoing security and integrity of County Government and public owned equipment, information and systems are not compromised.

6.6 Compliance with the following Public Internet Access Code of Conduct

The use of the County Government public internet access facility in libraries or public venues is provided on the condition that, compliance with the following Public Internet Access Code of Conduct is accepted.

The creation, accessing, copying, storing, transmitting or publishing of any material that:-

- 6.6.1** is sexually explicit or obscene is prohibited.
- 6.6.2** is racist, xenophobic, sexist, homophobic, defamatory, harassing or in any other way discriminatory or offensive is prohibited.
- 6.6.3** possession of which would constitute a criminal offence is prohibited.
- 6.6.4** is either criminal or illegal, or promotes criminal or illegal activities is prohibited.
- 6.6.5** contains images, cartoons or jokes that will cause offence is prohibited.

Notice is given that all activity and internet connections managed by the County Government are monitored and recorded.

Copies of the Public Internet Access Code of Conduct and advice below should be clearly displayed in areas where public access to the internet is made available.

6.7 Legal Framework Governing Public Internet Access

It is illegal to create, access, copy, store, transmit or publish any materials that fall into the following categories:-

- 6.7.1 National Security:** instructions on bomb-making, illegal drug production, terrorist or any other criminal activities.
- 6.7.2 Protection of Minors:** inappropriate forms of marketing, displays of violence or pornography involving minors

6.7.3 Protection of Human Dignity: incitement to tribal, xenophobic, racial hatred or racial discrimination, harassment.

6.7.4 Economic Crimes: fraud: instructions on pirating credit cards or financial systems.

6.7.5 Information Security: malicious hacking.

6.7.6 Protection of Privacy: unauthorised communication of personal data, electronic harassment.

6.7.7 Protection of Reputation: libel: unlawful comparative advertising.

6.7.8 Intellectual Property: unauthorised distribution of copyrighted works, e.g. software or music.

6.8 Terms and Conditions

6.8.1 In libraries, prior to use of the public internet service, users will be obliged to read and accept an on-screen version of the above code of conduct. Users should be aware that the County Government regularly monitors the use of public internet access facilities and the misuse of the facility could result in services being withdrawn or the content of an individual's activity being reported to the police.

6.8.2 All County Government owned equipment designated for use as public internet access systems are secured against theft and damage in accordance with the County Government's ICT Security policy, installed with malicious code protection software in accordance with the County Government's Malicious software and anti-virus policy and be recorded on the authority's asset database with a CG Register Item tag.

6.8.3 Any member of the public found interfering with either virus checking software, any other software, hardware or associated ICT equipment may be barred from subsequent use of any of the County Government's Internet service's ICT facilities.

6.8.4 The use of public internet equipment by County Government staff to process County Government information is prohibited, except in exceptional circumstances and with line management approval. *(See Also Chapter Third Party Connection and Acceptable use)*

6.8.5 Internet content viewed on CG owned equipment is passed through a filtering mechanism to control access to inappropriate information but the

County Government cannot be held responsible for that content. (See Also Chapter Access Control and Acceptable use)

- 6.8.6** Users should be aware that the Internet is not a secure medium and that third parties may be able to obtain information regarding user's activities.

- 6.8.7** Privately owned devices may be used to connect to filtered '_Guest' wireless access points at designated CG properties. No other method of connection is permitted from privately owned devices. (See Also Chapter on BYOD Policy)

- 6.8.8** Controls are implemented to prevent users of the public internet service accessing, installing software or additional hardware on County Government equipment. (See Also Chapter ICT Asset Management and ICT Equipment Use)

- 6.8.9** Controls are implemented to return County Government equipment to a default configuration on termination of a user session, including the removal of all personal identifiable data. (See Also Chapter Data Protection and Information Security)

- 6.8.10** County Government equipment available for use by the public will in future have hard drive access removed. USB ports and read/write CD and DVD drives are accessible but they are configured in such a way to stop software being installed onto the PC.

CHAPTER SEVEN

7. THIRD PARTY CONNECTIONS

7.1 Introduction

The County Government of Nyeri connections to Third Party organisations to promote partnership working, information sharing, service provision and support arrangements with Third Party organisations or service providers. This policy is specific to the County Government's requirements when establishing new links between the County Government and Third Party organisations and makes reference to additional County Government security policies and procedures.

7.2 Purpose

The purpose of this policy is to clarify the procedures and responsibilities with regard to initiating a new connection between the County Government and a Third Party organisation or service provider in order to maintain confidentiality, integrity and availability.

7.3 Scope

Third parties are defined as any individual or organisation not employed directly by the County Government and includes partners such as the parastatals, National Government organizations, Police and other authorities. It also includes suppliers and contractors who require access to the County Government's network to provide remote support.

This policy applies to all existing and new permanent or temporary connections and applies to any connection agreement with a third party. Any sanctions and obligations specified within the contract may be imposed as part of the third party connection agreement.

7.4 Third Party Compliance

The overall security of the County Government's infrastructure, systems and data takes precedence over any individual requirements for a Third Party connection.

A specific business purpose must exist and be defined for a Third Party connection to be considered. For each Third Party connection agreement, named lead persons responsible for the system and information concerned must be appointed by both the County Government and the Third Party.

7.5 Risk Assessment

A risk assessment should be conducted, prior to implementation of any connection, to identify specific requirements. It will be the responsibility of the named County Government lead person to carry out the assessment.

The risk assessment will consider:

- 7.5.1** A description of the participants in the assessment.
- 7.5.2** The type of access required and the data that needs to be available to the Third Party.
- 7.5.3** The value and sensitivity of information and information systems that may be exposed to unauthorised access.
- 7.5.4** The threat and vulnerability (the risk) to information and information systems and the impact if the threat were to take place.
- 7.5.5** The controls required to protect information and information systems.
An overview of the users.
- 7.5.6** How the Third Party organisation manages and controls information security.
- 7.5.7** Details of how the Third Party will secure their ICT equipment and networks.
- 7.5.8** The method of access required – physical and logical connectivity between information systems.
- 7.5.9** Dates and times of when the access is required from and a cessation date if a temporary arrangement. If a permanent arrangement is required, then an annual review must be incorporated in the agreement.

- 7.5.10** Security incident management.
- 7.5.11** Legal requirements affecting stakeholders.
- 7.5.12** A statement assessing and listing all risks.

Any Third Party Organisation with which the County Government enters into a connection agreement must be able to demonstrate compliance with the county's information security policies and enter into binding agreements that specify the performance to be delivered and the remedies available in the event of noncompliance.

7.6 Connection's Point of Contacts

The County Government point of contact will:-

- 7.6.1** Have administrative responsibilities
- 7.6.2** Draft a non-disclosure agreement in conjunction with the County Government's Legal Section for any/or named individuals accessing the services/information provided by the connection.
- 7.6.3** Be responsible for remote access provision
- 7.6.4** Act as a point of liaison both with the Third Party and The Directorate of ICT
- 7.6.5** Be responsible for ensuring background checks are made on individuals utilising services/information provided by the connection
- 7.6.6** Ensure all relevant bodies are informed when the connection is no longer required.

The Third Party point of contact will:-

- 7.6.7** Be responsible for managing all aspects of the connection on behalf of the Third Party
- 7.6.8** Be the primary point of contact and be able to provide accurate information on all aspects of the Third Party
- 7.6.9** Ensure that all Third Party users have received appropriate training and have undergone appropriate background checks.

7.7 Third Party Access Requirements

- 7.7.1** Third Party access to the County Government's network potentially exposes the County Government infrastructure to risk and therefore there must be an agreement in place that assures the County Government that any third party connection meets the County Government's security standards. The Third Party must consider and address:-

- a) A description of services and Service Level Agreement (SLA)
- b) Reference to relevant County Government security policies and legislation
- c) Requirements for asset protection and access control
- d) Responsibilities and liabilities
- e) Monitoring rights and reporting processes
- f) Conditions for termination and renegotiation of agreements

7.7.2 If a log of third party activity on the CG network is required as part of the agreement, then the third party will need to retain this log for the period specified in the agreement. Remote access software must be disabled when not in use.

7.7.3 All Third Party access must be facilitated through a method of connection approved by the County Government which provides protection to the satisfaction of the authority. All Third Party access must be logged via the IT Service desk and duly authorised before being permitted onto the County Government's network. Once authorisation has been obtained a time restrictive user name and password should be provided

7.7.4 Changes to methods of connection must be clearly defined and agreed by the County Government and the Third Party.

7.7.5 Third Parties and the County Government must inform each other about any security incidents which may impact on the confidentiality, integrity or availability of the third party service or data provided by the service. Incidents originating within the County Government must be handled in accordance with the 'Security incident management policy and procedures'. The range of security incidents which will require security awareness procedures include:-

- a) Computers left unlocked when unattended
- b) Password disclosures
- c) Virus warnings/alerts
- d) Media loss
- e) Data loss/disclosure
- f) Misuse/loss/corruption/alteration of Personal information.
- g) Physical security
- h) Missing correspondence
- i) Found correspondence/media
- j) Loss or theft of IT/information
- k) Misuse of IT equipment/facilities

7.7.6 Third Parties with whom the County Government has a Third Party connection contract are permitted access only to systems and information related to that contract. All other access is prohibited. Any Third Party with access to sensitive County Government information must be cleared to the same security and human resources checks as County Government staff.

7.8 Responsibilities

7.8.1 It is the responsibility of the County Government and each Third Party to ensure that all sections of this policy are adhered to.

7.8.2 Should changes in the requirements of either the County Government or the

Third Party regarding the connection become apparent, such as:-

- a) Life span of the service
- b) Changes in the information required
- c) Changes in the type of connection
- d) Changes in any aspect of security
- e) Changes of key contacts
- f) Emergency handling procedures

7.8.3 Each party should notify the other as soon as possible and the respective connection agreement should be revised.

7.9 Compliance with other Sections of the ICT policy

7.9.1 Several County Government non-ICT and Sections of the ICT Policy need to be considered as relevant within the sphere of any Third Party connection.

These include but are not exclusive to:-

- a) ICT Security
- b) Wireless Network
- c) Password Management
- d) Encryption
- e) ICT Acceptable Use
- f) Public Internet Access
- g) Security incident management policy and procedures

CHAPTER EIGHT

8. ICT ASSET MANAGEMENT AND EQUIPMENT USE

8.1 Introduction

The first Section of this chapter will handle ICT Asset Management and the Next Section will deal with ICT Equipment Use.

The County Government of Nyeri recognises the importance of ensuring its assets are identified, recorded and protected. The County Government is mindful to ensure all assets which it manages and owns are accounted for, maintained and controlled through the implementation of best practice, recording mechanisms, processes and procedures. Also, this chapter handles the ICT equipment Use within County Government Offices.

8.2 Purpose

The purpose of this policy is to ensure that all County Government of Nyeri's ICT assets are identified recorded and to establish professional good practice in the maintenance, protection and classification of all ICT assets.

8.3 Categorise of ICT Assets

The County Government categorises ICT assets as:

8.3.1 Information and Information Systems:

- a) Databases
- b) Data files
- c) Hardcopy documents
- d) User guides
- e) Training materials
- f) Policies, Procedures
- g) Business Continuity plans
- h) Financial Data

8.3.2 Software:

- a) Applications
- b) System software
- c) Development software
- d) Utility software

8.3.3 Physical:

- a) Computer equipment
- b) Communications equipment
- c) Media – storage and recording
- d) Property and accommodation

8.3.4 Services:

- a) Communications
- b) Utilities (power, lighting, environmental controls)

8.3.5 Personnel:

- c) Knowledge
- d) Skills
- e) Experience

8.3.6 Intangibles:

- a) Reputation

8.4 Scope

The scope of this policy extends to all County Government departments, employees, temporary staff, interns and students on attachment, contractors,

vendors and partner agencies who utilise or who are responsible for the development, management and maintenance of all County Government of Nyeri ICT assets

8.5 Policy Statement

The Directorate of ICT assumes 'nominated ownership' for the purpose of providing an 'entity' by which approved management responsibility may be controlled for all ICT Information and Data assets on behalf of the County Government. All identified ICT assets (which include hardware, software and licenses etc.) must be recorded in the County Government's ICT Asset Inventory. The County Government must take the following steps to ensure all assets are appropriately identified, recorded and maintained.

8.6 Information and Information Systems

8.6.1 Data and information held and maintained by the County Government can either be in hardcopy form stored in physical locations, filing systems, office locations or stored electronically using software and electronic backup systems.

8.6.2 The County Government's Electronic Document Management gives clear guidance and information on all aspects of storing information and data regardless of the form it takes.

8.6.3 Types of Information and Information Systems Assets:

- a) **Databases** – Access to these must be given to authorised employees only and logs should be maintained to record all access to and changes made to any data held within any database system
- b) **Data files** – Access to any data file(s) must be given to authorised employees only and logs must be maintained to record all access to and changes made to any data held within database systems
- c) **Hardcopy Documents** – All hardcopy documents containing sensitive and personal identifiable data must be accessed, processed, maintained and securely stored in accordance with the County Government's Information Safe Haven guidance. Restricted hardcopy documents requiring controlled access must have a signing in/out record maintained wherever appropriate
- d) **User Guides** – All user guides which assist and aid in the understanding of processes, procedures or systems should be safely stored and should be easily and readily accessible to all relevant employees – wherever possible. Guides which exist only in physical form should be digitised to include an electronic version which can be stored electronically on the

County Government's ICT Network and disseminated wherever possible on the County Government's intranet (NyeriNet)

- e) **Training Material** – All relevant training material(s) must be stored and made readily accessible to all relevant employees. Duplication or physical reproduction of training manuals must be kept to a minimum and avoided wherever possible
- f) **Policies, Procedures** – All County Government Policies and Procedures should be made available and disseminated via the County Government's Intranet (NyeriNet) – All original copies of Policies and Procedures documents whether electronic or hardcopy must be safely stored, regularly reviewed and a version history control record must be maintained for each document to ensure they are up to date
- g) **Business Continuity Plans** – All Business Continuity plans must be regularly reviewed, disseminated to appropriate employees and stored safely for easy retrieval as and when necessary
- h) **Financial Data** – Data and Information relating to County Government financial data must be restricted to authorised employees only. Recording mechanisms must be in place for logging access, changes and use of financial data and information

8.7 Software

Computer and IT systems software is widely used across the County Government and is vital to the day to day running of the County Government and in providing essential services to the public

The use of software has continued to change the way the County Government works. Substantial investment has been made in Software along with organization ongoing costs and expenditure such as annual software/systems support, licensing and staff training.

- 8.7.1 Applications** – Software used by the County Government must be appropriately sourced using approved supplier(s) and through the relevant laws and regulations governing procurement in the public sector and must be evaluated for business need, suitability, efficiency, ease of use, cost effectiveness and integration into existing County Government systems. All software approved for use by the County Government must be recorded on the Approved Software List. Appropriate numbers of software licenses must be purchased to cover volume of use and to satisfy legal requirements. Software media must be stored (physically and electronically) in a secure, centralised location (DML – Definitive Media Library) along with software installation codes

and registration numbers. Access to Software media/DML by employees must be controlled and limited to authorised employees only. A record must be maintained of all installations of software, licensing volumes SLA documentation and references in a centralised location (database) where access is provided to authorised employees only. A signing in/out system should be used for controlling the use of physical media.

8.7.2 System Software – Server/System software such as Operating Systems, must be evaluated for business need, suitability, efficiency, cost effectiveness and integration into existing County Government systems. Operating System installation media must be stored in a secure, centralised location (DML) along with installation codes. Access to server/system software media by employees must be controlled and limited to authorised employees only. A record must be maintained of all installations of software, licensing volumes SLA documentation and references in a centralised location (database) where access is provided to authorised employees only. A signing in/out system should be used for controlling the use of physical media. Backups of complete Server/systems installations must be routinely carried out for disaster recovery purposes. Installation, configuration and maintenance of Server/system software must only be undertaken by employees who are trained and qualified to do so

8.7.3 Development Software – such as RAD (Rapid Application Development) software for the support of existing systems and for the development of inhouse solutions must follow the same processes for procurement and use as for the Applications and Server/systems software. Development software should only be used by employees who are trained or who are undergoing training to use the Development software

All types of software (with the exception of routine security updates and patches verified by software vendors) must go through the Government procurement processes and must be recorded in the County Government's Approved Software list

8.8 Physical

The County Government's most visible assets are those which are physically located throughout the County Government such as computers, printers, tablets and phones, etc. Offices and buildings must also be considered as ICT assets – providing location for the housing and installation of the County Government's ICT Data and Communications Network infrastructure and physically stored documents and information.

8.8.1 Computer Equipment – A large number of computing devices - which includes PDAs, laptops, monitors etc., are in use across the County Government. Computers are one of the most costly single items of equipment and must be subject to controls from procurement to disposal. The County

Government must be able to track all activity and use relating to all County Government computing devices using various means such as via the computer network and/or using logging systems such as signing in and out and other such recording mechanisms. All computers must be allocated a unique asset tag number which is recorded against the manufacturer's serial number and model which should never be altered or exchanged with any other computer. Each computer must have the tag number securely located and easily visible on its outer casing along with the standard County Government security etchings. Throughout its life, a computer may be subject to hardware upgrades, new software installations, configuration changes and maintenance. All such activity must be recorded in the County Government's ICT asset management system which is maintained and updated by The Directorate of ICT

8.8.2 Communications Equipment – Mobile phones, office IP phones are widely used communications devices in use across the County Government of Nyeri. Other network and communications devices identified as assets include routers, switches, video conferencing equipment etc. Along with computing equipment, these devices must be allocated an asset tag number which is securely located and easily visible on the device. All communications equipment must be identified and recorded in the ICT asset management database

8.8.3 Media Storage and Recording – Media such as CDs/DVDs, Magnetic tapes, flash/portable hard disks are valuable assets because they are used to save and retrieve County Government information and data. The portable nature of this type of media requires responsible use and adherence to all policies, procedures and processes which are in place for the protection of information

and data. Appropriate labelling and recording mechanisms should be in place to ensure the safety and integrity of media - enabling tracking of essential media such as for data backups e.g. media required to carry out data/file restores must be signed in and out from a secure location. Portable media must be used in accordance with the County Government's encryption section of the ICT Policy, BYOD and Data Protection.

All physical computer, communications and storage media/devices must go through formal/legal purchasing procedures and must be recorded in the County Government's Approved Hardware list.

8.8.4 Property and Accommodation – The County Government's Corporate **Asset Management Plan** (This plan needs to be developed in collaboration with the department responsible for Housing) provides comprehensive information relating to buildings and property as assets. ICT equipment along with Data and Network Communications infrastructure equipment is housed in several buildings and property owned by the County Government and is therefore subject to the appropriate laws government laws and regulations.

8.9 Services

8.9.1 Communications – It is vital for the County Government to maintain its ability to communicate in many different forms. Communications equipment must be maintained and clear processes, policies and procedures for the provision of this service must be in place. E-mail is also a vital means of communication and as such, requires a robust, reliable infrastructure to enable the County Government to communicate effectively and reliably, both internally and externally

8.9.2 8.9.1 Utilities (power, lighting, environmental controls) – These services are assets as they provide fundamental requirements for the County Government to function appropriately, safely and effectively. It is essential that property maintenance and inspections are routinely carried out and that employees are proactive in reporting faults, whenever noted, to the department responsible for the management of public buildings.

8.10 Personnel

The County Government cannot function without its workforce – it is its largest asset. The provision of good public services requires government employees to have the necessary skills, knowledge and ability to work within many different areas and departments across the government. The number of unique functions and specialties across the government requires a varied knowledge and skills base which must be supported by robust recruitment processes, appropriate training provision and good management of employee skill identification, work placement and allocation of duties.

8.10.1 Knowledge and Experience – The County Government has a pool of employees who have a wide knowledge and experience base to draw on and is a valuable asset.

8.10.2 Skills – All County Government employees must possess the necessary skills and ability to do their jobs.

8.11 Intangibles

8.11.1 Reputation – The County Government is very aware that public perception and confidence in its ability to deliver effective, efficient public services is of the utmost importance. Reputation is an asset which promotes confidence and generates support in what the government is trying to achieve. The government takes its reputation seriously and proactively engages to develop policies and procedures along with a consistent approach in maintaining and presenting the right image.

The County Government encourages good reputation and is assisted by:

- a. Its Core Values:
- b. Good working practices:
- c. Corporate Image Branding:
- d. Public participation:

8.12 Information Classification

The County Government must develop an Information Classification scheme by which all ICT related assets are assessed and marked to indicate the level of criticality and sensitivity. Classification involves grouping information and categorising content to establish the most appropriate way of storage/retrieval and to determine who is authorised to access particular information and data. It is recommended that 'ownership' of this process should be the County Government's department responsible for ICT.

8.13 Acceptable Use of Assets

All County Government departments, employees, interns and students on attachment, contractors, vendors and partner agencies must observe and abide by the Acceptable Use Section of this Policy and procedures pertaining to government owned ICT assets. **See Chapter on Acceptable Use and the Section on ICT Equipment Usage.**

ICT Equipment Usage

8.14 Software: Software Installation

8.14.1 For purposes of complying with copyright laws and minimizing computer threats, only County Government authorised software must be installed on computers and this must be authorised by the Chief Officer responsible for Governors' Office or an appointed officer.

8.14.2 Computer users must not intentionally develop, use or distribute computer programs or software to disrupt other computer systems, information systems or damage software and hardware or bypass system security mechanisms and controls. More precisely, users must not use any software that may threaten the Confidentiality, Integrity and Availability of information and information systems. The use of any unauthorised or destructive program may result in legal civil action for damages or other punitive action by third parties, including County Government, as well as criminal action. Necessary disciplinary measures shall be instituted for staff who violate this policy.

8.14.3 All departments shall purchase computer hardware and software through the Directorate of ICT . These departments should clearly motivate the need for any special software or hardware.

8.14.4 Software under testing or evaluation must under no circumstances be installed on production computers including computers, laptops and servers. Evaluation software must be installed on IT equipment designated as test equipment and whenever possible separated from the production network. The Directorate of ICT has the sole authority to allocate ICT equipment for testing purposes.

8.15 Software Change Control

8.15.1 All software shall be held in a safe held at the Directorate of ICT.

8.15.2 Software taken from the cabinet by authorised staff shall be recorded in a software register and upon return be signed back into the register.

8.15.3 The Directorate of ICT shall license all appropriate software.

8.15.4 Should an officer require specialized software than currently available, the officer shall be required to request this in writing coupled with authorisation from the officer's supervisor? The Directorate of ICT shall evaluate the merits of each software request.

8.16 Reporting of Incidents

Illegal use of any software must be reported to the Directorate of ICT immediately. **See Chapter on Incident and Operation Management**

8.17 Computer Equipment: Protection of ICT Equipment Off-Premises

8.17.1 Users shall ensure that County Government ICT equipment is protected while in use away from County Government premises regardless of ownership. The security of the equipment should wherever possible be equivalent to on-site use of the equipment. The following applies to ICT equipment away from the office:

8.17.1.1 Users shall not leave ICT equipment unattended in public places;

8.17.1.2 By removing ICT equipment from County Government premises, users acknowledge the increased risk of theft and/ or loss, thus users must take all necessary precautions to protect and disguise these equipment. This can include using non-conventional laptop bags such as backpacks, securing them using laptop/projector locks and keeping equipment away from public eyes;

8.17.1.3 Only users who have been authorised to remove specific ICT equipment from the premises, shall be allowed to use the equipment off-site;

8.18 Equipment Change Control

8.18.1 All problems and changes to the computer equipment must be registered with the ICT Helpdesk.

8.18.2 No unauthorised staff may alter any software and hardware configuration.

8.19 Transfer of Equipment between Users

8.19.1 The transfer of ICT equipment shall be managed by Directorate of ICT and all requests for transfers has to be submitted to the Department of Governors' Office.

8.20 Standardisation of Hardware and Software

8.20.1 ICT personnel shall from time to time, ensure that ICT equipment in County Government is standardised as much as possible to minimise resources needed for maintenance, therefore users shall be required to comply with any recommendations as prescribed by Directorate of ICT .

Simply, this means that users will not bypass or attempt to bypass or disregard controls implemented by the department.

8.20.2 Additionally the department shall standardise computer software and hardware for users based on but not limited to job function, division and the least privilege principle. This will help avoid unnecessary software license costs.

8.20.3 Should a user require specialised hardware than the current standard, the user shall initiate this in writing. This must be authorised by the user's supervisor. The Directorate of ICT shall evaluate the merits of each hardware request.

8.20.4 Computer hardware shall only be modified by authorised ICT staff.

8.20.5 All computers must be installed with only the County Government's corporate antivirus software to protect against viruses and malicious computer programs. Users are prohibited from installation antivirus software or related software other than the corporate antivirus software from the Directorate of ICT.

8.21 Loss of ICT equipment

8.21.1 Lost ICT equipment shall be reported within 24 hours to the Chief Officer, Directorate of ICT , other than reporting the same to the Chief Officer of the respective department and to the relevant government agencies for action. Staff who lose ICT equipment assigned to them shall be required to replace the same at their own cost.

8.22 Unattended User Equipment

8.22.1 It is the sole responsibility of users to ensure the protection of ICT equipment which have been assigned to them by County Government. All laptop users shall be assigned with a laptop lock to prevent theft. Users shall ensure that they know how to physically secure their laptops. Offices, computer rooms and storage facilities shall also be locked when unattended. Failure to apply necessary protection for equipment shall constitute neglect and the user may be held liable for the loss.

8.22.2 Users shall terminate active sessions or log out of their computers when moving away from the workstation unless they lock the computer in which case they would be required to re- enter the password. No computer may be left unlocked.

8.23 Disposal and Reuse of Equipment

8.23.1 It may be necessary for the department to dispose of old or obsolete ICT equipment to make way for faster and more efficient computers. In this case The Directorate of ICT shall take the sole responsibility of ensuring that all licensed software is removed and all stored information is securely overwritten/erased. Any individual who disposes any ICT equipment without the secure removal of data will be exposing the County Government to compromise and unauthorised disclosure of information, thus will be in direct breach of this policy. **See Chapter on E-waste Management and Disposal**

8.23.2 In cases where previously used ICT equipment including laptops, personal computers or memory sticks are reassigned to another employee, The Directorate of ICT shall ensure that all information is securely deleted to protect the confidentiality of information

8.24 ICT Equipment by Category: Critical ICT Equipment

To ensure that critical business activities take place and to prevent loss, damage or compromise of critical assets, critical ICT equipment shall be protected from various security threats and environmental hazards. The following special controls shall govern the security of this critical equipment:

8.24.1 All critical systems such as servers, switches, routers or printers used to print confidential personal information shall be stored in a physically secure environment protected by access control.

8.24.2 Owners of critical ICT equipment shall implement the highest possible protection of these assets against failure, disaster, unauthorised access, tampering and periodically review security breaches and misuse.

8.24.3 Owners of critical ICT equipment shall keep updated copies of configurations, operational procedures and usage guidelines to ensure continuity of operations after failures and prevent a single point of failure wherever possible.

8.25 Laptops

- 8.25.1** In order to maximise use of resources, staff shall either be issued with a laptop or a desktop computer for official use.
- 8.25.2** Officials that have been allocated or provided with laptops shall be responsible for the safety and custodianship of the laptop in and outside the office.
- 8.25.3** On connection to a local area network (LAN), a notebook that has been out of office shall be automatically updated with the latest antivirus signature file by the County Government's corporate antivirus server. This is done in the background, and a user may not observe or be aware of this action.

8.26 Removable Media

Removable media such as memory sticks, DVDs and data compact discs are often the primary entry point of unauthorised software and viruses and a means of unauthorised information leakages. As a result the following guidelines shall be followed when using removable media;

- 8.26.1** Users shall always be required to scan removable media for viruses prior to use. This can be done simply by right clicking the removable media or CD icon in My Computer and selecting —Scan for viruses. Data on the media must only be accessed upon successful scanning and removal for viruses, if any;
- 8.26.2** Users shall take the principles of least privilege into consideration when copying official information and data to removable media. This means that users are not allowed to copy information which they are not authorised to access. Additionally, users must take all necessary precautions to safeguard all classified or unclassified official data residing on removable media from unauthorised access;
- 8.26.3** Copyright laws apply to copying of data to and from removable media. A user may be held liable for any copyright violations.

8.27 Printers

- 8.27.1** Users shall be required to share printers on the network based on physical proximity and section/department in order to avoid unnecessary costs.

8.27.2 Users of printers shall take into account that printer resources such as cartridges and paper are not infinite and refrain from misuse of printers by printing personal or unauthorised documents.

8.27.3 The Directorate of ICT shall ensure that all management interfaces of printers are protected by a password to prevent unauthorised use or configuration.

8.27.4 Recognising that documents can be processed and stored on computers, users shall take care to optimize printing resources by only printing when a paper copy is necessary.

8.27.5 Sensitive or classified printed documents shall immediately be removed from the printer after printing to prevent unwanted information disclosures.

8.27.6 Printers that are dedicated to printing confidential information such as pay slips, invoices and cheques shall be stored in areas where physical access is strictly controlled. These areas should be clearly marked to deter unauthorised access. It is the responsibility of each division to protect such sensitive printers.

8.27.7 Only authorised maintenance personnel shall carry out printer repairs.

8.28 Personal Use

While ICT equipment is allocated to ensure that users have the necessary tools to carry out their official duties, it is inevitable that equipment will be used for personal use. While this is not prohibited, the use of ICT equipment for personal use should be in a responsible manner that does not incur unnecessary costs to County Government. The following guidelines govern personal use of ICT equipment:

8.29 Equipment should not be used to process, distribute or store any data or information protected by copyright laws / or intellectual property rights as this can lead to legal action;

8.30 Computers must not be used to play games or perform any activities that may contribute to decreased employee productivity.

For more see chapter on BYOD of this ICT Policy

8.31 House Keeping

Users shall use County Government ICT equipment responsibly in line with the following housekeeping rules:

8.31.1 Offices with ICT equipment shall be locked when leaving the office to prevent theft amongst other things;

8.31.2 ICT equipment shall not be placed next to heaters or air conditioners as humidity and heat can shorten the life of internal computer components;

8.31.3 Users shall not eat, drink or smoke next to ICT equipment as this cause damage to the equipment and could be a health and safety risk;

8.31.4 Only damp cloths with suitable cleaning fluids shall be used when cleaning computer keyboards, screens, printers and other ICT equipment;

8.31.5 Whenever possible, ICT equipment shall not be connected to the same electric power as other power consuming devices. Red plugs should only be used for ICT equipment;

8.32 Movement of ICT Equipment to and from County Government Premises

8.32.1 ICT equipment shall not be moved from government premises without proper authorisation from the head of the department or unit. This authorisation shall be in the form of a duly signed prescribed form –Authority to remove Government equipment from Premises Form obtainable from from the Supply Chain Management section

8.32.2 All other ICT equipment taken into County Government premises shall be signed in.

8.33 Computer user's responsibilities

- 8.33.1** Users shall ensure proper use of ICT equipment in accordance with all provisions of this policy.
- 8.33.2** Users are required to report any misuse of ICT equipment or alert The Directorate of ICT of potential threats to ICT equipment.
- 8.33.3** It is the user's responsibility to seek guidance from The Directorate of ICT when in doubt of what constitute acceptable or prohibited use of ICT equipment.

8.34 Responsibilities fo The Directorate of ICT

- 8.34.1** The Directorate of ICT shall implement mechanisms and technological controls to ensure, monitor and enforce compliance to this policy.
- 8.34.2** The Directorate of ICT shall review this policy annually or when necessary to address new issues arising from the use ICT equipment.
- 8.34.3** The Directorate of ICT shall investigate and follow-up on reported and suspected non-compliance and take necessary corrective actions.

CHAPTER NINE

9. CYBER SECURITY

9.1 Introduction

This Chapter on Cyber Security of the ICT Policy is a formal set of rules by which those people who are given access to organization's technology and information assets must abide by.

The Cyber Security policy serves several purposes. The main purpose is to inform organization users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the organization. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

The Cyber Security section also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users of penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the organization organization's computer systems and networks.

9.2 What are we protecting?

It is the obligation of all users of the organization systems to protect the technology and information assets of the organization. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the organization are made up of the following components:

- 9.2.1 Computer hardware, CPU, disc, email, web, application servers, PC systems, application software, system software, etc.
- 9.2.2 System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- 9.2.3 Application Software: used by the various departments within the organization. This includes custom developed software applications, and commercial off-the-shelf software packages.
- 9.2.4 Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

9.3 Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The County Government shall classify the information it controls. The Chief Officer responsible for the Directorate of ICT is required to review and approve the classification of the information and determine the appropriate level of security to best protect it. Furthermore, the CO shall classify information controlled by units not administered by a CO.

9.4 Classification of Computer Systems

Security Level	Description	Example
----------------	-------------	---------

RED	<p>This system contains confidential information – information that cannot be revealed to personnel outside of the organization. Even within the organization, access to this information is provided on a –need to knowll basis.</p> <p>The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of the organization.</p>	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information.
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access Server and application(s). Management workstations used by systems and network administrators.
WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
BLACK	This system is externally accessible. It is isolated	A public Web server with non-sensitive information.

	<p>from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information.</p>	
--	---	--

9.5 Local Area Network (LAN) Classifications

A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one RED system and all network users will be subject to the same restrictions as RED systems users. A LAN will assume the Security Classification of the highest level systems attached to it.

9.6 Definitions

9.6.1 Externally accessible to public. The system may be accessed via the Internet by persons outside of the organization without a logon id or password. The system may be accessed via dial-up connection without providing a logon id or password. It is possible to —pingll the system from the Internet. The system may or may not be behind a firewall. A public Web Server is an example of this type of system.

9.6.2 Non-Public, Externally accessible. Users of the system must have a valid logon id and password. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or a private Intranet. A private FTP server used to exchange files with business partners is an example of this type of system.

9.6.3 Internally accessible only. Users of the system must have a valid logon id and password. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and it does not respond to a —pingll from the Internet. A private intranet Web Server is an example of this type of system.

9.6.4 Security Administrator. The Chief Officer for ICT shall designate an officer within the department as the Security Administrator for the County Government.

9.7 Threats to Security

9.7.1 Employees

One of the biggest security threats is employees. They may do damage to organization's systems either through incompetence or on purpose. Security has to be layered to ensure that this is compensated by undertaking the following:.

- a) Assigning appropriate rights to users. Access should be limited to working hours only. Ensuring that users do not share accounts. Users should NEVER share access information with co-workers.
- b) Revoking access to employees whenever they are moved transferred or retired from sections. .
- c) Keeping detailed system logs on all computer activity.
- d) Physically securing computer assets, so that only staff with appropriate need can access.

9.8 Amateur Hackers and Vandals

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favourite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

9.9 Criminal Hackers and Saboteurs.

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

9.10 User Responsibilities

This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the organization.

9.11 Acceptable Use

- 9.11.1** User accounts on organization computer systems are to be used only for business of the organization and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the organization computing system and facilities may constitute grounds for either civil or criminal prosecution.
- 9.11.2** Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the organization. (**See Also Chapter on Acceptable Use**)
- 9.11.3** Users shall not purposely engage in activities with the intent to: harass other users; degrade the performance of the system; divert system resources for their own use; or gain access to organization's systems for which they do not have authorization.
- 9.11.4** Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the organization IT designee.
- 9.11.5** Users are prohibited from downloading unauthorized software from the Internet onto their PCs or workstations.
- 9.11.6** Users are required to report any weaknesses in the organization computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

9.12 User Classification

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator. Furthermore, all users must conform to the Acceptable Use Chapter of this Policy defined in this document. The County Government has established the following user groups and defined the access privileges and responsibilities:

User Category	Privileges & Responsibilities
---------------	-------------------------------

Department (Employees)	Users	Access to application and databases as required for job function. (RED and/or GREEN cleared)
System Administrators		Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a –need to know basis only.
System Administrator	Security	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer/System Developer		Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
Contractors/Consultants		Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to organization information and systems must be approved in writing by the organization Head – ICT Systems or the Chief Officer responsible for ICT. See Third Party Connection Chapter
Other Agencies and Business Partners		Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.
General Public		Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information.

9.13 Monitoring Use of Computer Systems

The organization has the right and capability to monitor electronic information created and/or communicated by persons using County Government computer systems and networks, including e-mail messages and usage of the Internet. It is not the County Government policy or intent to continuously monitor all computer usage by employees or other users of the County Government's computer systems and network. However, users of the systems should be aware that the County Government may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line

length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with County Government policy.

9.14 Access Control

A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements. **See Chapter on Access**

Control

9.15 User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and **MUST NOT** be shared with management & supervisory personnel and/or any other employee whatsoever. **See also Network Security, Password Management and Acceptable Use Chapters of this policy**

CHAPTER TEN

10. SERVER SECURITY

10.1 Introduction

The County Government of Nyeri has a large and complex ICT infrastructure. Servers form a key part of this infrastructure - providing essential services, access to computer applications, security and data storage. The County Government's ICT network would be unable to function or provide its critical services without the availability of servers.

All administration, installation and configuration of servers and associated systems which form part of the County Government's IT infrastructure and which falls under the responsibility of the Server Room Server Support team must be undertaken in line with all existing County Government policies and procedures.

10.2 Purpose

The following details the security implications and measures required to ensure the County Government's server infrastructure is protected through effective and well managed procedures and practices.

10.3 Scope

This policy applies to all County Government servers which are maintained and installed within secure County Government buildings and locations. The County Government's main headquarters at Nyeri is the location for the Server Room. The Server Room houses most of the Server and Network equipment and serves as the main access area to the County Government's ICT Infrastructure

10.4 Policy Statement

The Chief Officer shall appoint a Server Room Manager who will manage the Server Infrastructure.

10.5 Server Room Manager Responsibilities

To secure the Server Rooms, the Server Room Manager must ensure that:

10.5.1 Appropriate mechanisms are in place to record the names, dates, times and signatures for the signing in and out of visitors (including County

- Government personnel) to the Server Room. All visitors must be issued with an authorised County Government visitors badge when signing in
- 10.5.2** Any visitors to the Server Room area must be accompanied at all times by authorised County Government personnel
 - 10.5.3** Any person not known to Server Room personnel must be challenged in order to establish who they are and whether authorisation has been granted to them to be there
 - 10.5.4** Access to and knowledge of door lock codes or access control mechanisms are restricted to authorised personnel only and must not be shared with any unauthorised person.
 - 10.5.5** Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the Server Room Manager in line with professional best practice and immediately when an employee (who has access to sensitive ICT areas) ceases to be employed by the County Government
 - 10.5.6** Electronic access tags must be issued to authorised staff on an individual basis. Staff issued with access tags must have their names and employee numbers recorded against the registered access tag number including date and time of issue
 - 10.5.7** Access tags should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorised personnel may be permitted to use another authorised person's tag if available with permission of the line manager and the recorded user must either be present or be made aware that their tag is being used. Any such use must be recorded and maintained in a logging system for this type of event
 - 10.5.8** Access to server rooms including any adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms
 - 10.5.9** Access tags issued to personnel who no longer work for the County Government must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system
 - 10.5.10** Doors which provide access to the Servers/rooms are not to be left/wedged open unless for the purpose of taking delivery of new equipment, to accommodate the movement of existing equipment, transportation of maintenance or cleaning equipment – an authorised member of staff must be present at all times to supervise access when doors are left open
 - 10.5.11** All County Government/Contracted Cleaners must have and display appropriate identification and be made aware of the requirements within this policy
 - 10.5.12** Personal, special access visits from relatives or acquaintances of personnel are not permitted to secure areas. There must be a valid reason

for all visits and any such visitors must go through the standard signing in/out procedure

10.5.13 Any issues to do with official authorisation of access to the Server Room Area should be sought from the Server Room Manager – in the absence of the Server Room Manager, clearance should be requested from the Assistant Director of Infrastructure or the Information Security Manager

All staff must abide by the Server Room's Physical Access Control Policy which is made available to Server Room personnel and can be requested from the Server Room manager

10.6 Environment

Servers are physically stored/located in the Server Room areas. The Server Room accommodates ICT infrastructure equipment from both the Server and Network support teams. Access to the Server Rooms given by personnel from either team to visitors must be formally authorised by the Server Room Manager as any access given will be providing access to both Server and Network infrastructure equipment. In the absence of the Server Room Manager, formal clearance must be requested from the Assistant Director of Infrastructure (Directorate of ICT) or the Information Security Manager.

The Server Rooms are sensitive ICT areas and as such, require a high degree of physical and environmental controls. The Server Room's **Physical Access Control Policy** describes these controls.

All authorised personnel must ensure that they comply with the policies, procedures and best practice specific to the Server Room working environment:

10.7 Configuration and Maintenance

The County Government's Network Domain IT Infrastructure is built on and around the Microsoft Windows environment. All Servers which include critical infrastructure functions (excluding any alternative/legacy Servers running disparate operating systems), are installed with Microsoft Windows Server based operating systems. Administration of these Windows based Servers is normally provided by a dedicated team of Server Support personnel.

Administration, maintenance and configuration of these Servers requires the following considerations in order to protect the security, integrity and reputation of the County Government:

- 10.7.1** All server hardware and software should be (or in the process of being) recorded on the County Government's approved hardware and software list
- 10.7.2** All server hardware and software should be purchased/obtained using approved vendors through the County Government's procurement procedures
- 10.7.3** Adequate levels of staffing should be provided at all times – particularly for call-out purposes or systems requiring out-of-hours support
- 10.7.4** All visitors, contractors or vendors carrying out hardware/software installations and/or maintenance should not be left unattended while working - unless authorised by the Server Room Manager or an appropriate supervisor. Access within the building should also be limited to areas where the work is to be carried out
- 10.7.5** Servers must be regularly updated with the latest Windows Operating System security updates and patches using Microsoft Windows update services
- 10.7.6** Servers must be protected from malicious software and viruses using industry standard antivirus and anti-malware software regularly updated with the latest definition and signature files whenever they become available
- 10.7.7** All Servers must record all logon, system and application activity via Windows event logs which must be archived off and stored securely elsewhere on a regular basis
- 10.7.8** All unnecessary Services, Applications, and Network Protocols should be removed or disabled
- 10.7.9** All unneeded or unnecessary Default Windows Accounts should be disabled
- 10.7.10** Backup and restore procedures and routines must be employed so that systems and data files can be restored and recovered in the quickest, most efficient time possible. *See Chapter on Information Backup and Recovery*
- 10.7.11** Disaster recovery procedures must be in place in the event of loss of Server(s) or IT infrastructure and procedural documentation must be regularly updated to include any changes/updates to existing procedures or processes involved. *See Chapter on Information Backup and Recovery*
- 10.7.12** Server/Domain Fault tolerance and Redundancy procedures should be in place and tested for effectiveness on a regular basis and procedural documentation must be regularly updated to include any changes or updates

- 10.7.13** Any new software or systems to be installed on the County Government's Servers must be provided with documentation detailing running environment specification, installation procedures and details of any known issues which could adversely affect the security and integrity of the County Government's Server infrastructure – these requirements must be formally identified and included in system documentation and service agreements on procurement of the software/system
- 10.7.14** Configuration changes to software, Servers and systems must be passed through the County Government's Change Advisory procedure and any planned work to be scheduled should include a notification to all parties affected via the Change Control Procedure
- 10.7.15** Emergency Changes will be reported to the CAB during working hours where appropriate. In out-of-hours emergency situations the Assistant Director (Infrastructure) or the Server Room Manager will use their professional judgement to decide on the appropriate course of action.

Back-up, Restore and Disaster Recovery procedures should be in place and made available at the Server Room.

10.8 Administrative Accounts

- 10.8.1** All Server support staff who are provided with Domain Administrator privileges must ensure at all times that individual passwords are not shared with anyone else – in line with the County Government's Password policy
- 10.8.2** Authorised personnel with Domain/administrative access to Servers and ICT devices must have their account disabled immediately on suspension or cessation of employment with the County Government
- 10.8.3** Authorised personnel with administrative access to Servers for maintenance, installation or configuration must logon with individual usernames and passwords wherever possible
- 10.8.4** All server support staff who are provided with Domain Administrator privileges must ensure their own account passwords are set to expire on a regular basis in line with existing account expiration policies and professional best practice
- 10.8.5** All accounts (other than individual user accounts) which are used solely for the installation, maintenance and configuration of servers, software and/or other supporting hardware equipment must be disabled prior to and after use – i.e. account only to be enabled when required
- 10.8.6** Groups and accounts added to local Server administrator or other privileged groups must be removed unless absolutely necessary – a record of Groups and accounts which are added to local Server Administrative/privileged groups must be maintained

10.8.7 All ICT devices which may require local logon privileges for configuration and maintenance i.e. SAN appliances etc... must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of the County Government's Password Section of the ICT policy wherever possible. **See chapter on Encryption and Password Management**

10.8.8 All server administrative, privileged, software systems account passwords (not individual user accounts) must be stored using encryption which utilises a minimum of 128 Bit AES encryption and must only be accessible to Server support personnel. **See chapter on Encryption and Password Management**

10.9 Service Accounts

Service accounts can be described as any account that does not correspond to an actual person. These are often built-in accounts that services use to access resources they need to perform their activities. However, some services require actual user accounts to perform certain functions.

The following considerations must be taken into account when working with service accounts and system services:

10.9.1 All services must be run using local/system accounts wherever possible

10.9.2 New software and systems procured must fulfil the requirement of using local/system accounts to run services wherever possible

10.9.3 All Domain accounts currently used to run services must have a password length and complexity in line with the County Government's password policy and professional best practice

10.9.4 Domain accounts which were configured to run a service/s but which are no longer required must be disabled and/or removed (deleted)

10.10 Remote Access

10.10.1 Procedures must be in place to ensure that any external remote connections enabled for third party software/system support to the County Government's Network/Servers are setup to connect via the County Government's (VPN) portal and any access via the old VPN service is disabled

10.10.2 The Server Support team must ensure that the correct procedures and processes are in place to facilitate and enable third party vendors to provide support for the County Government's software and systems using the most secure methods available

-
- 10.10.3** Access accounts used to provide third party support are only to be enabled when required and disabled immediately when not required including regular account password changes. Documentation detailing this process must be developed and disseminated to relevant areas such as The Directorate of ICT Service Desk in order to protect the County Government's Servers and network infrastructure
 - 10.10.4** The Server Support team should facilitate County Government staff accessing the County Government Network/Servers remotely and should be restricted to using the most secure protocols and tunnelling mechanisms available
 - 10.10.5** Server Support staff working remotely or from home must observe the same controls and procedures as when working within the County Government in order to ensure security and integrity and to prevent loss and/or damage to County Government assets and reputation

CHAPTER ELEVEN

11. PASSWORD MANAGEMENT

11.1 Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the government's entire corporate network. As such, all County Government of Nyeri employees, including partner agencies, contractors, volunteers and vendors with access to government's systems are responsible for taking the appropriate steps, as outlined below, to select, use and secure their passwords.

11.2 Purpose

The purpose of this Section of the ICT policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change across all Information and Communication Technologies (ICT) related systems throughout the County Government.

11.3 Scope

This policy applies to all employees, interns, contractors, volunteers, vendors and partner agencies who:

- 11.3.1 have or are responsible for any network account or resources (or any form of access that supports or requires a password) on any system that resides at any County Government facility.
- 11.3.2 have access to the County Government's data network.
- 11.3.3 store any non-public County Government information.

11.4 Policy Statement

With continuing reliance on ICT systems, it has become increasingly important to ensure the integrity of all system/access logon accounts used across the County Government is maintained. The following procedures and practices must be followed to ensure the security and integrity of these accounts.

- 11.4.1** All users must ensure that their password is not divulged or shared with anyone else.
- 11.4.2** All users must not write down and store passwords within the office i.e. in office diaries or paper files.
- 11.4.3** Passwords must not be inserted into email messages, SMS messages or other forms of electronic communication with the exception of some systems/processes which may require automatically generated temporary passwords to be sent. These temporary passwords must be changed as soon as possible.
- 11.4.4** All ICT devices which may require local logon privileges for configuration and maintenance i.e. Printers, network switches, routers, SAN appliances etc... must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of this policy wherever possible.
- 11.4.5** All ICT systems should:
 - a. Support individual user authentication – providing for identification of specific users and not just groups
 - a) Prevent the storing of passwords in clear text or in any easily reversible form
 - b) Provide for management of specific roles and functions within a system enabling delegation of tasks to individuals
 - c) Not contain or utilize embedded (hard-coded) passwords – these are passwords which are –fixed (saved) on a computer or device and are often –hidden from view. Embedded passwords can be used as a –back door to computers and systems and must be prevented.
 - d) Use access control procedures, which apply to both operational and test systems equally.

11.5 Domain Range

This policy relates to both the internal and external County Government of Nyeri domains to which employees, interns, contractors, volunteers, vendors and partner agencies logon. Specific configuration of enforced password policies for each domain is as follows:

11.5.1 Nyeri County Government Intranet (NyeriNet)

This domain services the County Government's main network and enables user logons and authentication. It is also the security boundary for the majority of systems in use and accessed by County Government employees, interns, partner agencies, contractors, volunteers and vendors.

Password configuration enforced by the default domain group policy for this domain:

- a) Enforce password history **10** passwords remembered
- b) Maximum password age **45** days
- c) Minimum password age **2** days
- d) Minimum password length **8** characters
- e) Account lockout threshold **5** invalid logon attempts
- f) Reset account lockout counter after **30** minutes
- g) Users are prompted to change password at logon **7** days prior to the existing one expiring.
- h) All systems SHOULD designed to log off if left idle for a period of more than one minute
- i) Passwords must meet complexity requirements – this forces the use of passwords which **MUST** contain at least three of the following five elements:
 - i. Numeric – (0-9)
 - ii. Uppercase – (A-Z)
 - iii. Lowercase – (a-z)
 - iv. Special Characters (? , ! , @ , # , % , etc...)
 - v. Spaces

11.5.2 External Connections

This domain services external (3rd party) connections to the County Government's network and facilitates external user logons and authentication. It is the security boundary placed between the Internet and the County Government's internal network. This domain boundary is used to contain user account logons for various parties including software support, interim access and the County Government's access accounts.

Password configuration enforced by the default domain group policy for this domain:

- a) Enforce password history **20** passwords remembered
- b) Maximum password age **30** days
- c) Minimum password age **1** days
- d) Minimum password length **8** characters
- e) Systems SHOULD be designed to log off if left idle for a period of more than 30 seconds
- f) Password must meet complexity requirements – detailed as above **11.5.1**
- g) Account lockout threshold **3** invalid logon attempts

All externally procured software must satisfy the requirement of this ICT policy

11.5.3 Responsibilities

Implementation and adherence to this policy is the responsibility of all County Government employees, interns, partner agencies, contractors, volunteers and vendors working for the County Government. It is important that every employee takes seriously, the use, protection and integrity of their own password/s or any other system password/s which they may be privy to from time to time and to encourage, guide and inform staff wherever possible for those who are responsible for the supervision of others.

11.6 Guidelines

11.6.1 General Password Construction Guidelines

Passwords are used for various purposes at County Government of Nyeri. Examples of some of the more common uses include: user level accounts, web accounts, email accounts, local access to ICT devices such as routers, printers etc. All staff should be aware of how to construct and select strong passwords.

Strong passwords have the following characteristics:

- a) Contain both upper and lower case characters (e.g., a-z, A-Z)
- b) Have digits, punctuation and special characters as well as letters e.g., 0-9, !@#\$%^&*()_+ | ~-=\`{}[]:;'"<>?,./)
- c) Are at least eight alphanumeric characters long.
- d) Are not a word in any language, slang, dialect, jargon, etc.
- e) Are not based on personal information, names of family, etc.
- f) Passwords should never be written down or stored online. Try to create passwords that can be easily remembered.

Poor, weak passwords have the following characteristics:

- a) The password contains less than eight characters and doesn't include any special characters or numbers
- b) The password is a word found in a dictionary (English or foreign)
- c) The password is a common usage word such as:
 - i Names of family, pets, friends, co-workers, fantasy characters, etc.
 - ii Computer terms and names, commands, sites, companies, hardware, software.
 - iii Birthdays and other personal information such as addresses and phone numbers.
 - iii Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - iv Any of the above spelled backwards.
 - v Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

11.7 Creating Passwords using Passphrases/Sentences

Using passphrases is a good way of constructing strong passwords and helps with remembering them. Passwords constructed in this way, will typically consist of letters, numbers and special characters which are used to represent the words or meaning of a phrase. The following example describes this process:

Example

Step 1 – Choose a phrase – for example: „*I catch the number 14 bus on Fridays*“

Step 2 – Use the first character of each word: I c t n 14 b o f

Step 3 – Mix with lower and uppercase letters: **iCTn14bOf**

Step 4 – Incorporate special characters (such as !@#\$%^&*()_+ | ~-=\`{}[]:;'<>?.,/) and numbers to increase complexity. Using this method, the final password could be: **i*CTn#14bOf5**

N.B. Incorporate special characters and numbers into your password in a way which helps you to remember where they should be e.g. could be after every 2nd, 4th, or 5th letter – or a similar ‘system’ which is meaningful to you.

Basically, the more letters, special characters and numbers used and the longer the password containing these is, the stronger the password will be.

IMPORTANT: The above passphrase/password is an example and must NOT be used.

11.8 Password Protection Standards

- a) Do not use the same password you use for County Government accounts as for other non-County Government access (e.g., personal ISP account, personal banking, online shopping, personal email accounts, etc.). Where possible, don't use the same password for various County Government access needs. For example, where applications don't utilise windows authenticated logons, choose different passwords for separate IT systems.

- b) Do not share your County Government's passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive and confidential County Government information.

List of "Don'ts":

- c) Don't reveal a password over the phone to ANYONE - unless relaying information on temporary passwords which are changed immediately
- d) Don't write passwords down and store them anywhere in your office
- e) Don't reveal a password in an email message - unless relaying information on temporary passwords which are changed immediately
- f) Don't reveal a password to your line manager
- g) Don't talk about a password in front of others
- h) Don't hint at the format of a password (e.g., "my family name")
- i) Don't reveal a password on questionnaires or security forms
- j) Don't share a password with family members
- k) Don't reveal a password to co-workers while on holiday

11.9 Additional Information

- l) If someone demands a password, refer them to this document and request that they call the ICT Service Desk.
- m) Do not use the "Remember Password" feature of applications (e.g., on web browsers such as Internet Explorer, Mozilla Firefox, etc...).
- n) Do not store passwords in a file on ANY computer system (including mobile devices or similar) without encryption.
- o) Change passwords at least once every 30 days (with the exception of systemlevel passwords which must be changed quarterly). The recommended change interval is every four months.
- p) If an account or password is suspected to have been compromised, report the incident as soon as possible to the Service Desk or via one of the other methods as described in the County Government's Security

Incident Management Policy and Procedures. Immediately change any/all passwords which may have been compromised.

- q) Password cracking or guessing will be performed on a periodic or random basis during audit penetration tests involving 3rd party companies. If a password is guessed or cracked during one of these scans, the user will be required to change it immediately. All audit penetration tests must be approved by the Chief Officer responsible for Governors' Office prior to the work commencing.

11.10 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- a) Should support authentication of individual users, not groups.
- b) Should not store passwords in clear text or in any easily reversible form.
- c) Should provide role management functionality, such that one user can take over the functions of another without having to know the other's password.
- d) Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

CHAPTER TWELVE

12. ENCRYPTION

12.1 Introduction

The protection of electronic information and access to storage systems is vitally important - especially with the ever increasing, greater demand on the use of ICT systems across the County Government of Nyeri. Protecting person identifiable and business critical information from unauthorised access, disclosure or loss whether by theft or accident is of paramount importance.

A secure, robust ICT infrastructure along with appropriate policies and procedures will help to ensure that wherever possible, all steps have been taken to protect this information.

Encryption technologies provide a level of protection for the storage, transmittal, retrieval and access to this data. Encryption works by converting data to make it inaccessible and unreadable to unauthorised individuals. The only way to read the encrypted data is by using a decryption key.

The Kenya Information and Communication Act of 2009 requires the County Government to have appropriate policies and procedures in place to ensure the safe keeping, use, retrieval and access to data covered by the Act. The County Government has a responsibility to ensure the integrity, security and protection of all data which it holds.

12.2 Purpose

The purpose of this policy is to:

- 12.2.1** Detail the specification and deployment of data encryption software for the protection of electronic information held by the County Government
- 12.2.2** Provide guidance on the responsibilities of the use and handling of portable media
- 12.2.3** Provide clarity on the types of portable storage and mobile devices which are allowed for use
- 12.2.4** Describe how encryption will be used and applied to devices
- 12.2.5** Provide guidance on the responsibilities of the use of encrypted devices
- 12.2.6** Detail the method of reporting breaches of this policy whether intentional or accidental

12.3 Scope

This policy covers all electronic data and details the types of devices which are acceptable for the storage / transmittal of data, and how these devices utilise encryption software - irrespective of whether or not the data held on them is considered sensitive or confidential.

This policy covers encryption for the following devices and applications:

- 12.3.1** Desktop, laptop, tablet computers
- 12.3.2** Handheld devices such as mobile phones, tablets and PDAs
- 12.3.3** Portable storage devices e.g. USB memory sticks, external drives
- 12.3.4** Removable media e.g. floppy disks, DVDs/CDs, backup tapes
- 12.3.5** Email

The County Government's –Acceptable Use section of this ICT Policy provides more general information on the e-mail service and use and is available from the County Government's intranet, (NyeriNet).

12.4 Policy Statement

Full disk encryption will be rolled out gradually to all computers across the County Government.

The encryption software employed for use at the County Government uses the **AES 128 bit** (Advanced Encryption Standard) which is a symmetric-key encryption with a 128 bit key.

12.5 Application

12.5.1 Full disk encryption will be rolled out to all desktop computers by the ICT Support as part of desktop upgrades. All County Government laptops should be encrypted.

12.5.2 The County Government data should not be stored on computers or portable media devices unless access is required when network connectivity is not available. When it is necessary data should only be stored on authorised devices.

12.5.3 Encryption is applied to all authorised data storage devices attached to desktop, laptop or tablet computers. In certain cases, it may not be feasible for certain devices to be encrypted and each exception to a device will be given full and careful consideration as to its use and any decision made will be based on best practice and business need.

12.5.4 Where exceptions have been identified for not encrypting specific devices, computer policy settings (enforced at domain level) which enable/disable encryption can be applied individually to a specified computer and/or groups of computers.

12.5.5 When a portable, County Government recommended data storage device is used, the instructions for the correct use must be followed to ensure the data is encrypted.

12.5.6 Personal storage media and equipment must not be connected to the County Government's network and must not be used to store County Government data. **(Refer to BYOD Chapter)**

12.5.7 Other portable USB devices include mobile phones, cameras, PDAs etc. These other devices should not be used to store County Government data. You must contact the ICT Support Centre if you need to use these devices as part of your job.

12.5.8 If clarification is needed as to the recommended USB data storage devices allowed for use, the ICT Support Centre should be contacted.

The ICT Support Centre will advise on the best method to encrypt individual files.

12.6 Method

On encryption of an authorised portable storage device (e.g. USB data stick) the user will need to set a password for accessing the device. The password for encrypted portable devices must be in line with the County Government's password policy and be enforced at the domain level. Using the portable device on any other computer after being encrypted will require a password in order to access it. It is important that local procedures are put in place to ensure that passwords used to encrypt devices are approved by line managers, so that in the event an individual leaves the County Government, access can be gained to the data. In the event that local procedures for the creation of encryption passwords have not been followed, employees may be asked to provide details of encryption passwords used on all such portable devices. **Under no circumstances should network or other IT system passwords be disclosed to anyone including the ICT Support.**

The use of DVD/CD devices and floppy drives will be restricted to read-only access – this will be enforced at the domain level by Group Policy.

Where there is a need for a particular job function requiring write access to CD/DVD or floppy drives, this can be enabled as an exception and recorded formally with agreement from the Directorate of ICT . Any agreement to allow write access of CD/DVD or floppy devices will include the conditional use of appropriate 3rd party archiving (zip) compression/encryption software to be used to encrypt any data stored or written to these devices. This conditional encryption/compression software will be made available as recommended by the Directorate of ICT .

Any other requirement for portable storage device such as portable hard drives, magnetic/DAT tapes and devices must be discussed with the ICT Support and only hardware and software on the County Government's approved software and hardware list is to be used.

12.7 Responsibilities

The County Government has a responsibility to provide its employees with the appropriate secure storage mechanisms, procedures, devices and software for the secure handling, storage and retrieval of all electronic data held by the County Government. The use of portable devices may be subject to random periodic review by the County Government to ensure compliance with the encryption policy.

All County Government employees, elected members, volunteers, partner agencies, contractors and vendors have a duty to abide by all policies and procedures to ensure the safe, secure handling of all electronic data.

12.8 Use of portable storage media and devices

County Government employees, partner agencies, contractors and vendors undertaking work for the County Government who are issued with portable storage devices, writing to portable storage media, viewing / transmitting encrypted data or accessing have a responsibility to ensure:

- 12.8.1** No one other than authorised person/s are aware of the encryption/decryption password for the device, media or system.
- 12.8.2** Any portable device or media is not given to any unauthorised persons for safe keeping
- 12.8.3** Any portable device or media is not left discarded or unattended in a public place
- 12.8.4** All reasonable steps are taken to ensure that during transit, any portable device/media is locked via a key or combination lock and securely located. Portable devices/media must not be left unattended in any vehicle at any time due to insurance requirements
- 12.8.5** Any portable device or media is adequately protected from physical damage
- 12.8.6** Any portable device or media is not hired, lent out or given without authorisation from the Directorate of ICT .
- 12.8.7** Any portable device or media which is no longer required or has reached its lifespan must be handed over to the Directorate of ICT. All

data on the device / media must be wiped, destroyed and disposed of through the County Government's ICT disposal procedure

12.8.8 The device / media is handed back to your line manager or the ICT Support on cessation of employment with the County Government

12.8.9 The device / media is handed back to your line manager or the ICT Support when no longer authorised to use the device / media

12.8.10 The loss of any portable device is notified immediately via the County Government's Security Incident Management procedure.

CHAPTER THIRTEEN

13. SECURE DESK/DATA PROTECTION

13.1 Introduction

Information, in whatever form it takes, is a valuable asset to the organisation and consequently needs to be suitably protected. Protecting information is not only a corporate responsibility; it is also a responsibility which all staff including Elected Members, partners, vendors and contractors, working in or for County Government of Nyeri must take seriously.

The Secure Desk Policy supports the ICT Security Policy and other related policies.

13.2 Objectives

13.2.1 The objective of this policy is to ensure that all paper and electronic records containing person identifiable information, or any other confidential/sensitive information (including corporate or commercially sensitive information) is suitably secured when not in use and is not left visible on an unattended desk.

13.2.2 This policy applies in particular to working areas, such as desks or tables, which should not have confidential, sensitive, commercially sensitive or person-identifiable information left on them whilst unattended for an extended period.

13.2.3 The objective of this policy is also to ensure that the County Government adheres to the obligations placed upon it by the Data Protection Act 1998 as well adhering to the County Government of Nyeri Code of Conduct.

13.3 Key Principles

The key principles of adhering to the Secure Desk Policy are listed below:

13.3.1 To reduce the risk of a security breach or information theft;

13.3.2 To reduce the risk of confidential or sensitive information / documentation being stolen or accessed by unauthorised individuals which could damage the integrity of County Government of Nyeri;

13.3.3 To help demonstrate compliance with the Kenya Information and Communication Act of 2009;

13.3.4 To create a culture of staff responsibility in relation to the handling and care of personal data and other confidential information;

13.4 Definitions

13.4.1 Personal Data

Personal data is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name, private address, home telephone number, National Insurance number etc.

For example this could include printed spreadsheets of staff and payroll details or address files.

13.4.2 Sensitive personal data

Sensitive personal information is where the personal information contains details such as that person's:

- a) Physical or mental health condition
- b) Sexual life
- c) Ethnic origin
- d) Religious beliefs
- e) Political views
- f) Criminal convictions
- g) Membership of a trade union

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

13.4.3 Corporately and Commercially Sensitive Information

Corporately and commercially sensitive information may, through improper disclosure, cause reduced competitiveness or breach procurement practices.

Such information may include building leases, commercial / third party contracts or internal plans.

13.5 Scope

It is the responsibility of those listed below to ensure they adhere to the Secure Desk Policy across County Government of Nyeri

13.5.1 All County Government employees

13.5.2 All contractors and vendors

13.5.3 Partner agencies using County Government of Nyeri premises

13.5.4 All visitors using the —hot desk areas

13.5.5 Interns and students on attachment

The policy applies to all staff in all the organisation's locations, irrespective of area of work or discipline.

The policy applies to desks, tables, computer screens, photocopier, fax and printer areas.

13.6 Responsibilities

13.6.1 All employees, contractors, elected members and agency staff are required to comply with the Secure Desk Policy.

13.6.2 Line managers are responsible for monitoring compliance and providing guidance to staff on the implementation of the policy.

13.6.3 All employees, elected members, contractors and agency staff have a responsibility to report security incidents and breaches of this policy as quickly as possible via the County Government's Incident Reporting Procedure.

The County Government will take appropriate measures to remedy any breach of the Secure Desk Policy through the relevant framework in place. In the case of an employee, then the matter may be dealt with under the County Government's disciplinary process. Internal reviews by management and Internal

Audit, including spot checks will take place in order to identify potential breaches of this policy.

13.7 Secure Desk Procedure - Protecting Data and Information

Confidential or sensitive information, whether held electronically or on paper records and other valuable resources should be secured appropriately when staff are absent from their workplace and at the end of each working day.

To facilitate this, the following guiding principles have been produced which cover both non-electronic (e.g. manual/paper files) as well as electronic forms of information.

In addition reference is made to the display of information on the computer / laptop screen as well as to the security of personal property.

13.7.1 Desks must be cleared at the end of each working day of any confidential or person identifiable information. Files containing confidential information must be locked securely in desks, filing cabinets or designated secure rooms at all times, other than when being used by staff. All efforts must be made to keep this information secure and not readily accessible to non-authorized staff.

13.7.2 To reduce the risk of a breach of confidentiality and adherence to the Data Protection Act, when disposing of person identifiable information, ensure that it is destroyed securely using approved methods of waste disposal. *(See E-Waste and Disposal section of ICT Policy).*

13.7.3 Personal items (i.e. keys, handbags, wallets etc) should be locked away safely in the interests of security. It is the responsibility of the owner to ensure all security precautions are taken.

13.7.4 Health & Safety – desks and other work spaces should be sufficiently tidy at the end of each working day to permit the authority's cleaning staff to perform their duties.

13.8 Electronic Storage Devices

For the purposes of this policy electronic data and equipment will **not** be treated differently from manual records and equipment, if they contain the same type of confidential, sensitive and/or personal information. Computing and all other equipment containing data will therefore be treated with the same level of security as paper based resources.

13.8.1 To ensure the security of information held electronically, lock away portable computing devices such as Laptops or PDA devices when not in use and where appropriate;

13.8.2 To ensure the security of information held on mass storage devices such as CDROM, DVDs or USB drives, lock these away in a secure drawer at the end of the working day;

13.8.3 13.8.1 USB drives and other such items must be locked away even if they are encrypted.

13.9 Personal Computers, Laptops and Personal Digital Assistants.

13.9.1 Computers and laptops must not be left logged on when unattended. When staff have to leave their desks for any reason, they must lock the computer by using the '_Control, Alt, Del' keys simultaneously or by pressing the '_Windows' key and the letter '_L'. Access to the computer/laptop must be protected by passwords.

13.9.2 As far as practicable, when sensitive or confidential information is being worked on, the window must be closed or minimised, or the computer locked when unauthorised persons are in close proximity to the screen.

13.9.3 If sensitive or confidential information is visible to an unauthorised person standing in close proximity to computer/laptop screen, they could be asked to move away to protect the confidentiality of this information.

See Also Chapter on BYOD

13.10 Printers, Photocopiers and Scanners

13.10.1 Where there is a shared printer or multi-functional device available, all printing should be locked by default, requiring the users to enter a 4 digit PIN to release their documents.

13.10.2 To avoid accidentally printing to an unintended network device, computer users should additionally check that their default printer is correct before printing any documents.

13.10.3 Personal data must be cleared from printers, photocopiers and fax machines immediately on completion. If these are no longer required the items must be shredded or sent for secure disposal.

13.10.4 It is the responsibility of the person who sends information to be printed to ensure they collect their documents. All documents should be sent to print using the locked print facility. If information is of a confidential/sensitive nature and it is misplaced or missing, this should be logged as an incident on the Security Incident Form on Dnet.

CHAPTER FOURTEEN

14. DESKTOP PC SECURITY

14.1 Introduction

The County Government of Nyeri is reliant on the use of ICT equipment across all areas of the organization. Devices such as desktop, laptop, notebook and tablet PCs are provided for use by those who require them to carry out their duties. PCs are also made available for use to members of the public for access to information, resources and County Government services. The County Government and its employees have a duty to ensure that appropriate levels of security are applied to all PCs used in the office environment..

The purpose of these procedures is to ensure that PCs in an office environment are used, configured and managed in a secure and safe way and to identify and describe the steps required to achieve and maintain this

14.2 Procedures

ICT equipment such as desktop, laptops, notebooks and tablet PCs are all capable of being used in the office environment over long periods on a daily basis.

The scope of these procedures cover:-

- 14.2.1** Any desktop, laptop, tablet, notebook (mobile device) PC configured with a windows operating system and has a desktop image Provided by DCC
- 14.2.2** Predominantly used in the office environment
- 14.2.3** That is or can be connected to the County Government Network.

Access to computers and devices must be controlled using secure methods and procedures in order to prevent damage to County Government assets and reputation.

Normal, everyday use of PCs provided by the County Government for potential use within the office environment requires the following security considerations:

14.3 Commissioning and replacement:

- 14.3.1** All requests for the purchasing new Desktop PCs are placed through The Directorate of ICT except for a few exceptions e.g. schools, specialist educational equipment.
- 14.3.2** Every new PC ordered from the approved County Government supplier is provided with a County Government asset tag number – this number is used to name the PC and is also recorded against the computer for any fault calls or installation/maintenance requests made through the Service Desk or call logging system.
- 14.3.3** Except where a workplace assessment or business need dictates otherwise, computers are replaced using the ‘_standard’ approved hardware and software specification as identified by and existing on the approved software and hardware list created by Directorate of ICT & eGovernment.
- 14.3.4** All new PCs are marked using etching type stencils with the name –County Government of Nyeri and the identification asset number" (or

as may be prescribed from time to time) on both the PC monitor (screen), main computer case mouse and keyboard.

- 14.3.5** The computer asset number is recorded in the central hardware inventory database. The life of the PC from commissioning to disposal must be tracked and recorded.

14.4 Configuration

All County Government PCs are supplied to users with a preconfigured standard Windows Operating System image which The Directorate of ICT has developed.

Differing departmental requirements result in department specific applications being layered on top of the standard image. In terms of security; all computers connected to the County Government's County Government network domain will all have the same level of security applied across all areas.

All County Government Desktop PCs are subject to the following configuration which ensures PCs are added to the County Government network and have the correct security configuration settings applied:

- 14.4.1** All County Government PCs use the Microsoft Windows family Operating System – Currently Windows 7, with the emphasis on and movement towards Windows 10 only.
- 14.4.2** New Desktop PCs will have the approved –standard Windows image loaded from Microsoft System Configuration Manager by The Directorate of ICT PC Commissioning Unit. The configuration of the Desktop image deals primarily with the –look and feel of Windows and some changes which may be necessary for optimisation of the operating system.
- 14.4.3** PCs can only be added to the Nyeri County Government Domain and a computer account created by an authorised Directorate of ICT & eGovernment account that has sufficient access permissions to do so'
- 14.4.4** Newly commissioned Desktop/laptop/tablet PCs are added to the County Government Domain using an asset tag number with a prefix relevant to the type of PC.
- 14.4.5** PCs can only be added to the Domain and configured with a computer account, by Directorate of ICT staff who are authorised and have sufficient access permissions to do so. Authorised staff are required to logon –locally to the PC using the built-in Administrator's account in order to add the computer to the Domain. During the process of adding the computer to the Domain, authorised staff are required to provide a valid County Government account username and password to complete the process

- 14.4.6** County Government PCs are protected from viruses and spyware/malware using **approved antivirus** , virus definition files will be released across the network as and when required
- 14.4.7** Following the adding of a PC to the Domain, the security settings for the PC are applied and enforced automatically, immediately on –boot-up of the computer. These security settings are applied and enforced at the Domain level using Windows Group Policy which will override any changes made locally on the PC
- 14.4.8** The locally Built-in administrative passwords on the PC are changed automatically by Group Policy (on boot-up) once it is added to the Domain
- 14.4.9** The locally Built-in Administrative groups on the PC are propagated by all the relevant Directorate of ICT network groups and users who require admin privileges e.g. Area Support, Support Desk etc – including some departmental network groups which have been approved and authorised to be added
- 14.4.10** Users who have an account within at least one of the groups added to the local administrator's group will be provided with full administrative control of the computer but will not be able to override the settings which have been applied by Group Policy
- 14.4.11** Desktop PCs which are for use in public access, residential/care or partner agency areas are subject to the same security restrictions enforced by the County Government's network domain. Any network accounts used to access these PCs are managed and authorised by The Directorate of ICT
- 14.4.12** Screen savers and desktop will be supplied and approved by Directorate of ICT team and cannot be changed by users

***N.B.** Desktop PCs which have not been provided by the County Government but have been approved for use will be subject to the relevant security checks and procedures by the Directorate of ICT and Complies with the BYOD Section of this policy*

14.5 Location

Desktop/laptop/notebook/tablet PCs which are used by County Government employees, elected members, partner agencies, contractors and vendors are located across many sites and buildings.

The wide nature of access to many of these buildings and locations requires increased vigilance and awareness of the need for Desktop PCs to be secure and protected from unauthorised access, theft, physical damage and tampering.

Care and professional judgement to protect information and data should be taken in using computers which are located and positioned where:

- a) PC screen/s may be visible to members of the public/service users
- b) There is a danger of physical damage to a PC e.g. dropping, water, electrical
- c) PCs may be subject to interference e.g. strong electromagnetic sources
- d) PCs may easily be picked-up and/or stolen in obscured, low visible, nonstaffed areas

It is important to observe and maintain the physical security of rooms and offices where PCs are located.

County Government employees, elected members, partner agencies, contractors and vendors must be mindful of the potential for unauthorised access and viewing of County Government data and Information by members of the public/service users and take appropriate steps to avoid or prevent this in line with the County Government's Safe Haven Guidance

14.6 Use

County Government PCs may only be used by authorised parties for authorized

County Government business or purposes in accordance with the County Government's Acceptable Use Policy and associated security policies

All users of County Government Desktop/laptop/notebook/tablet PCs must ensure at all times that:

- 14.6.1** Account logon and system passwords are kept private and not shared, displayed or communicated to anyone else
- 14.6.2** County Government information and data must not be saved to PC hard drives – in the event of the County Government network being unavailable, advice should be sought from the Directorate of ICT
- 14.6.3** Sensitive and personal data must not be saved on the PCs hard drive under any circumstances
- 14.6.4** Data and Information saved to portable devices via a PC must only be copied to a portable device which is encrypted in accordance with the County Government's Encryption Policy
- 14.6.5** Screens/computers must be locked by users when away from the computer

- 14.6.6** PCs are not removed from their location without line management and/or approval from The Directorate of ICT
- 14.6.7** Unauthorised, non-standard equipment is not plugged-in or inserted into the computer
- 14.6.8** Software is not installed on the PC by unauthorised staff – any software installed must be (or going through the process of being) placed on the approved software list
- 14.6.9** PCs must not be mishandled, wilfully damaged or tampered with in any way – this includes taking off the PC case cover, or removing of any screws or fixings
- 14.6.10** Any suspicious or unknown equipment near or around PCs is reported to The Directorate of ICT
- 14.6.11** PCs are logged off and shut down when not in use for extended periods (i.e. overnight) and monitors are powered off

Note:

Any warnings visible on screen from the Anti-Virus software about identified/detected threats from viruses/malware should be reported to the Directorate of ICT & eGovernment Service Desk

14.7 Maintenance

- 14.7.1** All PC maintenance whether routine or major is carried out by Directorate of ICT authorised staff and our authorised third parties
- 14.7.2** Only staff working within an ICT function (or persons authorised by the Directorate of ICT) may perform maintenance, install applications/software or make system configuration changes to PCs. Staff may occasionally be requested to assist while under the supervision and authorisation of The Directorate of ICT as appropriate
- 14.7.3** A standard base configuration is installed on all County Government PCs. Any variations and additions must be agreed by The Directorate of ICT and the Security/Business Continuity Manager
- 14.7.4** PCs are protected against malicious code in accordance with the County Government's Malicious software and anti-virus Procedure
- 14.7.5** PCs are maintained in accordance with all relevant County Government policies and procedures

14.8 Disposal

The County Government shall operate a 5 year PC replacement programme. Computers which reach or exceed the 5 year term can, if required, be scheduled for replacement and disposed of through the Government's ICT

disposal procedures and as per the national procurement and disposal laws and regulations in place. **See E-Waste Management and Disposal Chapter of this Policy**

CHAPTER FIFTEEN

15. ELECTRONIC RECORDS MANAGEMENT

15.1 Introduction

The County Government of Nyeri acknowledges that as part of the corporate roll out of the County Government's Electronic Document and Records Management System (EDRM) in the near foreseeable future, it is likely that large series of paper documents will be scanned and added to the system to improve access and workflows. The County Government needs to be able to demonstrate that these scanned documents have been unaltered since the time of electronic storage and that they are a true representation of the original paper record. After scanning records and uploading them to the EDRM, departments/sections may wish to destroy the original paper file (However, there is need for legislation on the retention of electronic records) and use the scanned version as the definitive record for operational and compliance purposes.

The disposal of original paper records (and subsequent reliance on a scanned version) is a relatively recent concern and there is, as yet, no definitive case law on the subject of the legal admissibility of scanned files after the destruction of the paper original. However increasing numbers of public authorities are choosing to scan and destroy paper documents.

This policy sets out the arrangements required in the scanning and disposal process for scanned records in order to reduce the risk of a challenge to the legal admissibility and evidential value of the scanned records. This policy should conform with National Laws on admissibility of electronic records

15.2 Roles and Responsibilities

It is the responsibility of departmental and service managers to approve the scanning of documents and the destruction of the paper original, unless the original has to be returned to a third party or has to be retained for specific reasons because it is important to retain a wet signature. It is also the

responsibility of all managers to ensure that staff are made aware of the proper procedures to follow.

It is the responsibility of all staff involved in the scanning process to follow the agreed procedures for scanning.

It is the responsibility of all staff involved in the destruction process to ensure it is carried out in accordance with the principles of the County Government's E-waste and Disposal section of the ICT Policy. The main concern being that the original paper records are treated as **confidential waste**.

15.3 Scope

This policy applies to all staff who are involved in the scanning of records. Responsibilities under this policy include all stages of the scanning process including the preparation, scanning and filing stages.

For the purposes of this policy when a document has been scanned and the original paper copy destroyed, the scanned version will be regarded as the definitive record for legal, accountability and transparency purposes. The scanned copy will need to be managed in accordance with the County Government's Records Management and Records Disposal policies including retention of the digitised document for the agreed retention period.

15.4 Legal Framework

This policy seeks to address the key legal issues regarding the scanning and destruction process in terms of the legal admissibility and evidential weight of the digitised images.

As a general principle the action of copying a document may reduce its evidential weight. In order to respond to this there needs to be sufficient authentication evidence available to reassure legal and regulatory stakeholders that the image is an accurate copy. This will often require evidence that the document is what it claims to be and that it is a true and accurate copy, including proof that it has not been altered since the date it was added to a County Government approved electronic record keeping system.

See Chapter one under Legal Framework

As outlined under Section 15.1, a risk assessment approach is required for scanning initiatives, which should include assessing the likelihood of future legal

reliance on the scanned images. Where the legal risks are high then the use of the County Government's off-site document storage contract should be considered.

15.5 Policy Statements

The County Government is committed to the management of electronic information as outlined in the County Government's Information Security Policies including its Corporate Records Management Policy.

The County Government is committed to the continued use of electronic systems in the form of its Electronic Document and Records Management System for the storage of records over time. This system will be one of the County Government's primary systems used for the storage of digitised documents to ensure their authenticity and reliability.

The County Government is committed to consulting with key stakeholders to ensure that the systems used for the storage of digitised documents meet their needs in respect to compliance with legislation and regulations.

15.6 Policy Principles

The framework outlined under BS10008:2008 shall be complied with during scanning initiatives in order to maximise the evidential weight and legal admissibility of the scanned documents. Adherence to the following principles will enable the County Government to demonstrate its approach to scanning if the legal admissibility of scanned documents is questioned. If the scanning conforms to the principles outlined within this policy and associated procedures it will be acceptable to destroy the paper original and regard the electronic copy as the definitive record.

15.7 Procedures

General scanning procedures have been produced as part of the EDRM roll out which meet the requirements of BS10008:2008. These procedures should be followed in all instances where scanning takes place in order to maximise the legal admissibility of those resulting scanned records. It is essential that these procedures be followed regardless of whether departments are intending to destroy the paper originals. This is because if decisions over destruction occur after scanning, it is the scanning process itself which will raise legal admissibility questions.

15.8 Risk Assessment

In addition to adhering to the procedures developed by the ICT Team another requirement in any scanning initiative is to undertake a risk assessment with regards to the potential issues that might arise from a scanning project. This risk assessment should address the risk of a legal challenge, the risk of human error in the scanning process, the risk of technological failure and obsolescence and the risk of the alteration and manipulation of the scanned image. A template for a risk assessment exercise can be found in Appendix B.

15.9 Stakeholder Consultation

As part of the risk assessment process key stakeholders should be contacted prior to undertaking the scanning and destruction of originals. This should include contacting those stakeholders who are likely to be in a position of requesting access to scanned records (e.g. HR for finance related records).

There may be some cases where certain stakeholders feel that it is essential to retain the paper original, examples might include deeds to property, or documents with seals etc. to denote authenticity. The majority of records can be scanned with no need to retain the original, however in these minority of cases proper arrangements should be made to ensure the storage of the paper copy (for example using the County Government's approved supplier of off-site document storage).

15.10 Documentation

As part of the auditable scanning and disposal procedures authorisation for the destruction of the paper originals following scanning shall need to be obtained from the relevant head of service. This level of authorisation is only required for destruction occurring after a scanning initiative. Routine destruction of time expired records should be carried out according to the County Government's Record Disposal Policy.

Documenting the destruction shall require confirmation that the scanning process has been carried out in accordance with appropriate EDRM procedures. A destruction authorisation document can be found in Appendix C. This documentation will need to be retained for the duration of the retention period for the records which have been scanned as outlined in the appropriate departmental records retention schedule.

15.11 Review and Monitoring

A review of this policy will take place at least every two years to take into account changes in legislation and best practice.

On-going monitoring of this policy will be the responsibility of departmental Heads of Service, in consultation with the Corporate Records Manager, to ensure that the principles of the policy are being adhered to.

CHAPTER SIXTEEN

16. INCIDENT AND USER SUPPORT MANAGEMENT

16.1 Introduction

County Government of Nyeri is responsible for the security and integrity of all data it holds. The County Government must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to the County Government's assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security:

16.1.2 A computer security incident is an event affecting adversely the processing of computer usage. This includes:

- a)** Loss of confidentiality of information
- b)** Compromise of integrity of information
- c)** Denial of service
- d)** Unauthorized access to systems
- e)** Misuse of systems or information
- f)** Theft and damage to systems
- g)** Virus attacks
- h)** Intrusion by humans

16.1.3 Other incidents include:

- i)** Loss of ID badge/s
- j)** Missing correspondence
- k)** Exposure of Uncollected print-outs
- l)** Misplaced or missing media
- m)** Inadvertently relaying passwords
- n)** Loss of mobile phones and portable devices

Ensuring efficient reporting and management of security incidents will help reduce and in many cases, prevent incidents occurring.

16.2 Purpose

The management of security incidents described in this policy requires the County Government to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

The purpose of this Chapter of the ICT policy is to:

- a) Outline the types of security incidents
- b) Detail how incidents can and will be dealt with
- c) Identify responsibilities for reporting and dealing with incidents
- d) Detail procedures in place for reporting and processing of incidents
- e) Provide Guidance

16.3 Scope

This policy applies to:

16.3.1 County Government employees, elected members, partner agencies, contractors, volunteers and vendors

16.3.2 All County Government departments, personnel and systems (including software) dealing with the storing, retrieval and accessing of data

16.4 Policy Statement

The County Government has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing County Government employees, elected members, partner agencies, contractors, volunteers and vendors of the importance of the identification, reporting and action required to address incidents, the County Government can continue to be pro-active in addressing these incidents as and when they occur.

All County Government employees, elected members, partner agencies, contractors, volunteers and vendors are required to report all incidents –

including potential or suspected incidents, as soon as possible via the County Government's Incident Reporting procedures.

16.5 Types of Incidents

The types of Incidents which this policy addresses include but is not limited to:

16.5.1 Computers left unlocked when unattended

- a. Users of County Government computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All County Government employees, elected members, partner agencies, contractors, volunteers and vendors need to ensure they lock their computers appropriately - this must be done despite the fact that County Government computers are configured to automatically lock after 10 minutes of idle time.
- b. Discovery of an unlocked computer which is unattended must be reported via the County Government's Incident Reporting procedures.

16.5.2 Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, The Directorate of ICT must be notified through the County Government's Incident Reporting procedures. For more information, the County Government Password policy is available on the intranet (NyeriNet), main County Government website or via the Directorate of ICT 's Service Desk. Under no circumstances should an employee allow another employee to use their user account details – even under supervision.

16.5.3 Virus warnings/alerts

All Desktop, laptop and tablet computers in use across the County Government have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen.

The message may indicate that a virus has been detected which could cause loss, theft or damage to County Government data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to The Directorate of ICT Service Desk as soon as possible.

16.5.4 Media Loss

Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device (including portable media) who has misplaced or suspects damage, theft whether intentional or accidental must report it immediately through the County Government's Incident Reporting procedures.

16.5.5 ID Badges

It is essential for us to identify individuals and wearing ID badges helps us to do this.

16.5.6 Data loss/Disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- a) Transmitted over a network and reaching an unintended, unauthorised -recipient (such as the use of e-mail to send sensitive data)
- b) Intercepted over the internet through non secure channels
 - c) Posting of data on the internet whether accidental or intentional
 - d) Published on the County Government's website and identified as inaccurate or inappropriate
 - e) Conversationally – information disclosed during conversation
 - f) Press or media – unauthorised disclosure by employees or an ill-advised representative to the press or media
 - g) Data which can no longer be located and is unaccounted for on an IT system
 - h) Unlocked and uncollected print-outs from Multi-Function Devices (MFDs)
 - i) Paper copies of data and information which can no longer be located
 - j) Hard copies of information and data accessible from desks and unattended areas

All County Government employees, elected members, partner agencies, contractors, volunteers and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of County Government data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using the County Government's Incident Reporting procedures

16.5.7 Personal Information Abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc... must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information. Any abuse/misuse of such person identifiable information must be reported through the County Government's Incident Reporting procedures.

16.5.8 Physical Security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower floor/level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the Directorate of ICT via the County Government's Incident Reporting procedures.

Continuing emphasis and re-enforcement of the County Government's Secure Desk policy will further help to reduce the number of security incidents.

16.5.9 Logical Security / Access Controls

Controlling, managing and restricting access to the Authority's Network, Databases and applications is an essential part of

Information Security. It is necessary to ensure that only authorized employees can gain access to information which is processed and maintained electronically.

16.5.10 Missing Correspondence

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc... must be reported through the County Government's Incident Reporting procedures.

16.5.11 Found Correspondence/Media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through the County Government's Incident Reporting procedures.

16.5.12 Loss or theft of IT/Information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc... or which is known/or suspected to have been stolen needs to be reported immediately through the County Government's Incident

Reporting procedures

16.6 Responsibilities

It is the responsibility for all County Government employees, elected members, partner agencies, contractors, volunteers and vendors who undertake work for the County Government, on or off the premises to be proactive in the reporting of security incidents. The County Government's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of County Government data and information.

It is also a responsibility of all individuals and handlers of County Government data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

CHAPTER SEVENTEEN

17. INFORMATION BACK UP AND RECOVERY

17.1 Introduction

The County Government of Nyeri has a duty to ensure that all information and data which it is responsible for is securely and routinely backed up. The County Government has a responsibility to ensure that information and data which has been backed up can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances.

17.2 Purpose

The purpose of this policy is to identify and establish processes, procedures and good working practices for the backup and timely recovery of the County Government's information and data existing in both electronic and physical form.

17.3 Scope

The scope of this policy extends to the back-up of all important information and data regardless of the form it takes - including the recovery of IT systems and supporting infrastructure.

17.4 Policy Statement

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practice.

The following steps will help ensure the County Government's information and data is backed up and restored securely in the most efficient manner possible:

17.5 ICT Systems/Data Backups

- 17.5.1** The County Government's IT administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed in line with the County Government's Disaster Recovery Procedures and data retention policies
- 17.5.2** All IT backup and recovery procedures must be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery.
- 17.5.3** All data, operating systems/domain infrastructure state data and supporting system configuration files must be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration
- 17.5.4** All backup media must be encrypted and appropriately labeled with date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should be kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster
- 17.5.5** A recording mechanism must be in place and maintained to record all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc...) including any failures or other issues relating to the backup job
- 17.5.6** Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed
- 17.5.7** Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised
- 17.5.8** Access to the on-site backup location and storage safe must be restricted to authorised personnel only
- 17.5.9** All backups identified for long term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media
- 17.5.10** Backup media must be protected in accordance with the appropriate data protection and media handling procedures.
- 17.5.11** Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by the County Government's ICT systems. Where this may not be possible, photocopies of paper files must be made and stored in a secure storage location

- 17.5.12** Regular tests must be carried out to establish the effectiveness of the County Government's backup and restore procedures by restoring data/software from backup copies and analyzing the results. The Chief Officer – Governors' Office
- 17.5.13** The ICT Support should notify the Chief Officer – Governors' Office when backups fail – providing information such as the backup job detail and reasons (if applicable) for the failure. A record must be maintained, detailing the backup job failure including any actions taken
- 17.5.14** Backup data/media no longer required must be clearly marked and recorded for secure disposal and with due environmental consideration (Waste, Electrical and Electronic Equipment - WEEE Directive)

17.6 User Responsibilities

IT Users also have a responsibility to ensure County Government data is securely maintained and is available for backup:

- 17.6.1** IT Users must not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorized software which require the '_caching' of files locally in order to function). Instead, Users must save data (files) on their allocated areas – this could be an area within the EDRM system, a mapped drive or network shared folder the User has access to. Data (files) which are stored –locally will NOT be backed up and will therefore be at risk of exposure, damage, corruption or loss.
- 17.6.2** If the County Government network becomes unavailable for whatever reason and data or work is at risk of being lost, users have no option but to save the data (files) locally (i.e. on the computer being used) or on approved media storage such as a County Government owned encrypted Data stick (USB storage). Once the Corporate Network becomes available again, data (files) should be immediately transferred to the corporate network (Intranet) in order for it to be backed up safely and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored
- 17.6.3** Only County Government authorized encrypted USB data sticks should be used and any data stored must be for temporary purposes. All sensitive, business and personal identifiable information should be removed from the USB data stick and moved to an

appropriate County Government data network location as soon as possible in order to ensure the data is made available to the County Government and can be successfully backed up

- 17.6.4** Mobile phones must not be used to store sensitive, business or personal identifiable information. In the event of unforeseen or unavoidable situations leading to important data being stored on mobile phones, the data must be stored to a suitable County Government network location and removed from the phone as soon as possible.

17.7 Data Restores

The County Government should establish backup and restore routines.. Data (file) restores should be carried out by the Server Support Team who will endeavour to restore files from a date specified by the user or from the nearest backed up date.

- 17.7.1** IT Users must request data (files) to be restored by contacting the IT Service Desk. Only files which the user is authorised to access will be provided from the restore
- 17.7.2** The IT Service Desk will need to verify that the User has permission and/or authorisation to view or obtain restored copies of file/s and/or folder/s
- 17.7.3** Users requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:
- a) The reason for the restore
 - b) The name of file/s and/or folder/s to be restored
 - c) Original location of file/s and/or folder/s - the Service Desk will provide guidance to the User on how to find this out
 - d) Date, day or time of deletion/corruption or nearest approximation
 - e) The last date, day or time which the User recalls the data (files) being intact and accessed/used successfully
- 17.7.4** All backup and recovery (restore) procedures must be documented and made available to Server Room personnel responsible for carrying out data (file) restores
- 17.7.5** Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing or other unforeseen circumstance should be made under the

supervision of the Server Support Team via the County Government's IT Service Desk

17.7.6 Personnel accessing backup media for the purpose of a restore must ensure that any media used is returned to a secure location when no longer required (applies to media from both County Government and remote storage locations)

17.7.7 A log must be maintained to record the use of backup media whenever it has been requested and/or used from secure storage

The Server Room is a sensitive area and specific technical information regarding the detail of backup and restore procedures is held by the Server Room Manager

CHAPTER NINETEEN

18. WEBSITE

18.1 Introduction

The County Government of Nyeri has a duty to ensure to pass information to its citizenry through various channels including on its Website. The Official County Government Website shall be <http://www.nyeri.go.ke>

18.2 Scope

This policy applies to all the County Government Websites.

18.3 Purpose

This policy is designed to ensure that all County Government websites and digital services measure customer satisfaction, respond to the needs of their customers, and adapt to improve the delivery of those services based on customer feedback.

18.4 Customer Service

The County Government uses the Internet to share valuable content and resources with its customers. In order to ensure that the Department's digital presence continues to be of value, it is critical that Public Relations unit measure customer satisfaction by listening to the needs of their customers and adapt accordingly. Furthermore, the Digital Government Strategy requires agencies to implement common performance and customer satisfaction metrics for all national executive branch .go.ke Websites.

18.5 Content for Web Privacy Policies

The following items must be added as part of each operating unit's public-facing Privacy Policy in any instance when Web measurement and customization technologies are used:

- a. The purpose of the Web measurement and/or customization technology.
- b. The usage tier, session type, and technology used.
- c. The nature of the information collected
- d. The purpose and use of the information.
- e. Whether and to whom the information will be disclosed.
- f. The privacy safeguards applied to the information.
- g. The data retention policy for the information.
- h. Whether the technology is enabled by default or not and why.
- i. How to opt out of the Web measurement and/or customization technology; it is essential that this process be transparent and easy to follow.
- j. A statement that opting out still permits users to access comparable information or services.
- k. The identities of all third-party vendors involved in the measurement and customization process.
- l. If Tier 3 technologies are employed, the policy must refer to the fact that public notice and comments were sought. Also note that the Chief Officer for Governors' Office should provide written approval for the use of Tier 3 technologies on the Web site.

18.6 Content Management

County Government web pages are viewed by the public and employees as being the official position of the Department and have a high degree of visibility. It is imperative that Web content be overseen by management to ensure its quality, relevance to the agency's mission, and that it is delivered in a usable and accessible form.

The Chief Officer Governors' Office, through the Webmaster, is ultimately responsible for the content on Web sites of his or her organization and for its delivery. Therefore, managers should establish guidelines for the approval of Web content and its delivery.

18.7 Privacy Policy Statements and Information Collection

18.7.1 Privacy Policy

1. Major points of entry and any page where information is collected on any County Government's Web site shall include a clearly identifiable link to a privacy policy statement which shall disclose the information collection practices of the site. This link must be called "Privacy Policy."
2. In addition to disclosing the information collection practices of the site, all Privacy Policy statements must notify web site visitors of their rights under the relevant national legislation, regardless of whether the web site uses or collects any Privacy Act information, or any information at all.

18.7.2 Contents of the Privacy Policy Statement

1. General Privacy Policy Statement Requirements: The Privacy Policy statement shall cover each of the following elements, if applicable:
 - a) The kinds of information collected, including but not limited to email, data from forms, and information automatically collected by the server that administers your Web site.
 - b) How long the information is retained,
 - c) How it is used,
 - d) The conditions under which the information may be shared,
 - e) Who it might be shared with,
 - f) The conditions under which the information may be made available to the public, and
 - g) Whether information is collected from children.

The phrase "...conditions under which the information may be shared" refers to the possible sharing of information with other government entities. The phrase "...conditions under which the information may be made available to the public" refers to the potential availability of the information to the public or to private sector entities, such as pursuant to a Freedom of Information Act request or the sale to commercial entities. These instances must be clearly disclosed.

2. **Email and Persistent Tracking Technology:** In all cases, the Privacy Policy statement shall specifically address:
 - how email is handled, and
 - the use of "cookies" and other persistent tracking technology, and the extent to which information gathered this way is safeguarded.
3. **Management, Operation, Technical Controls and Safeguards:** The Privacy Policy statement must include, in clear language, information about management, operation, and technical controls ensuring the security and confidentiality of personally identifiable records, and, in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems (while not compromising security).

For sites that do *not* collect Privacy Act information, this requirement can be met by statements such as the following:

We collect no personally identifiable information about you when you visit our site unless you choose to provide that information to us. For the protection of users of our Web sites, we have safeguards in place to identify and prevent unauthorized attempts to access or cause harm to information and systems.

4. **Rights under the Kenya Information and Communication Act 2009:** All Privacy Policy statements must notify Web site visitors of their rights under the Privacy Act.
5. **Rights under Other Privacy-protecting Laws:** For units of the Department which are subject to other privacy-protecting laws in addition to the Privacy Act, and which therefore must also notify Web site visitors of their rights under those laws, the additional notification can be done in the body of the Privacy Policy statement, or via link to the specific applicable privacy regulation, or via link to other official summary of statutory rights.
6. **Collection of Voluntary Information – Additional Requirements:** When an agency Web site requests that a user provide voluntary information, and assuming the proposed collection of information is permissible, the Web site must *explicitly* inform the user that providing the information is voluntary. The Privacy Policy statement must inform users how to grant consent to use of voluntarily-provided information. In most cases, this can be done by a general statement such as, for example: "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose."
7. **Collection of Mandatory Information – Additional Requirements:** When an agency Web site collects mandatory information, and assuming the collection of information is permissible, the Privacy Policy statement must inform users how to grant consent to use of mandatorily-provided

information for other than statutorily-mandated uses or authorized routine uses under the Kenya Information and Communication Act 2009.

8. **Collection of Information Subject to the Kenya Information and Communication Act 2009 – Additional Requirements:** The Act covers any "system of records," i.e., any group of "records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

When a Web site collects information subject to the Act, it must explain what portion of the information is maintained and retrieved, in the Kenya Information and Communication Act 2009, System of Records, by name or personal identifier; and it must provide a Privacy Statement either at the point of collection, or via link to the applicable Privacy Policy statement.

When multiple Privacy Statements are incorporated in a Web Privacy Policy, a point-of-collection link must connect the Privacy Act Statement pertinent to the particular collection to which it applies.

Privacy Statements must notify users of the authority for and purpose and use of the collection of information subject to the Kenya Information and Communication Act 2009, regardless of whether providing the information is mandatory or voluntary, and of the effects of not providing all or any part of the requested information.

18.7.3 Location of the Privacy Policy Link

Where Web forms are used, a link to the Privacy Policy statement shall be viewable without scrolling, OR located adjacent to the "submit" button on the form. When multi-page forms are used, a link shall be viewable without scrolling on the first page AND adjacent to any "submit" buttons.

18.7.4 Note on Shared Privacy Policy Statements

Some links take users to separate Web sites within the same organization. There is a concern that different information collection practices may then apply. Therefore, when the information collection practices of various Web sites differ within the same organization the Privacy Policy statement of the parent organization should contain language similar to:

18.7.5 This Privacy Statement applies only to this Web site.

Any page where information is collected: The phrase "any page where information is collected," as used in this policy is a plain English term intended to be all inclusive and is not limited to personally identifiable information.

18.8 Using Information

We will never sell or share personal information with third parties. We may use this information to serve those users who have requested to be mailed with issues that we feel they may be interested in, such as website and organization news. Cookies are used for internal research and to give a better understanding of our audience.

You should also be aware that if you link out to third party websites, they have their own privacy policies for which we can accept no responsibility. Please be certain to check other sites before use.

18.9 Cookies

A cookie is a harmless piece of information that a website transfers to the cookie file of the browser on your computer's hard drive. On visiting the website, a cookie will be placed on your computer automatically by the website. We may use two types of cookie from time to time: —persistent cookies and —session cookies. Session cookies are temporary cookies that remain in the cookie file of your browser until you leave the website and persistent cookies are cookies which remain in the cookie file of your browser for much longer (though for how long will depend on the lifetime of the specific cookie).

We use cookies for monitoring load balancing between its servers while you are linked to the website, to conduct analyses of user traffic, and to perform web log audits. Third party advertisers may serve cookies via this website but these are only used to serve advertisements from the website's ad servers and to track whether these advertisements are clicked on by visitors to the website. We may pass the nonpersonal information collected by its cookies to third parties but only for the purposes of carrying out such monitoring, analysis or web log auditing, or for the purposes of tracking the number of anonymous users of the website.

Most browsers accept cookies automatically but you have the ability to accept/decline cookies by altering the settings in your browser. If you decline/disable cookies, you may not be able to use all the interactive features of the website or the website may not be available to you.

18.10 Security

The website is protected against unauthorised access using the latest security devices and firewalls.

18.11 Changes to the Privacy Policy

We reserve the right to add to or change the terms of this Privacy Policy in our sole discretion, without prior notice to you. If we change this Privacy Policy, we will post the new Privacy Policy on the website, and it will become effective from the time of posting to the website. Please visit this Privacy Policy on a regular basis to make sure you have read the latest version and you understand what we do with your information.

CHAPTER NINETEEN

19. SOCIAL MEDIA

19.1 Introduction

Social media and Web 2.0 (SM/W2.0) services are an increasingly important way for government staff to interact in an efficient, effective, and transparent manner with all those who are affected by or have an interest in government services, programs and activities.

SM/W2.0 services use many technologies, including XML feeds, wikis, blogs, social networking sites, discussion forums, collaborative research, web sites, comment features on news and video Web sites, and other mechanisms. Social media services allow the user to interact directly with the Web site or other users. The result is that Web users are able to communicate simultaneously, directly, and instantaneously with all other users on the Web site. Commonly used social media services include YouTube®, Flickr®, Facebook®, Twitter®, and WordPress®.

SM/W2.0 technologies also present new and unprecedented challenges to the security of the information technology (IT) networks and systems that County Government and its operating units use, as well as the privacy of personally identifiable information (PII) County Government maintains. County Government and other National Government information systems are targeted by persistent, pervasive, and aggressive threats. The threats may be directed against the network or system infrastructure, the records or information in the system, especially PII or other sensitive information. IT security controls currently in place may effectively protect County Government information systems as presently configured, but the rapid development of Web 2.0 technologies and their emerging capabilities and uses present new and ever increasing risks that require continuing vigilance by IT security personnel and employees who use SM/W2.0 services.

The purpose of this policy is to provide guidance for operating units and County Government employees to take full advantage of SM/W2.0 technologies while, at the same time, protecting County Government and its employees by mitigating the risks inherent in using these services without the proper safeguards.

19.2 Responsibilities of Managers

Before any SM/W2.0 service or technology is approved for use on any County Government network or system, the responsible operating unit Chief Officer

(CO)/Chief Information Officer/Public Relations Officer/Social Media Manager, using established risk management methodologies, must conduct a risk-based assessment to determine whether the users in the operating unit should be allowed to access the particular SM/W2.0 technology, and whether any limitations on access or usage are warranted.

The risk assessment conducted by a Chief Officer applies only to the operating unit for which the CIO is responsible. Depending on the level of IT security measures in place, a SM/W2.0 service may be approved for use on one operating unit network or for access from one operating unit system but not others. The Chief Information Officer (CIO) is responsible for maintaining a current inventory of SM/W2.0 technologies approved for access from their operating unit network(s) and systems.

Before authorizing employees to post information on a social media site, the Social Media Manager must verify that the SM/W2.0 service provider terms of service agreement has been approved by the County Government.

The CIO or Social Media Manager may allow employees to access a site for which there is not an approved terms of service agreement provided that the service provider does not require users to agree to a terms of service agreement for access to the site.

The CIO or Social Media Manager is responsible for oversight and monitoring of implementation of this policy by.

19.3 General Guidelines for the Use of SM Technologies in an Official Capacity

The following are general guidelines for Social Media Manager employees assigned official responsibility for operating an official account or contributing to a SM/W2.0 Web site, whether that site is hosted internally by the County Government (or an operating unit) or an external commercial service, on behalf of the County Government or an operating unit.

1. County Government employees using SM/W2.0 technologies in an official capacity must do so only on County Government-approved accounts and may only use official e-mail or other contact information for the creation and management of those accounts. In addition to helping the County Government keep track of how many accounts it has, using County Government-approved accounts will ensure that the County Government knows who is responsible for each account it uses. In the case of services that do not require accounts for the creation of a

County Government presence, employees should follow the service-specific guidance available on the County Government Website.

2. In general, County Government employees may only post from County Government-approved accounts information that represents official agency positions (i.e., not personal opinion). However, if a posting concerns a fundamental research communication as defined by the County Government Public Communications Policy and the posting is likely to be misinterpreted as an official County Government position, County Government employees must clearly state that they are providing their own personal opinions and not those of the operating unit, the County Government, or the Federal Government.
3. County Government employees should conduct themselves in a professional, courteous, and honest manner in all public communications about or related to their Government work, whether on-line, in person, at public meetings, or in other settings.
4. When posting a comment related to County Government work to a public Web site, County Government employees must identify themselves with their County Government affiliation and/or official title.
5. Posted information should be as accurate as possible. Although there is often a trade-off between speed of communication and accuracy, employees speaking in an official capacity should take reasonable steps to ensure that the information that they provide is correct, and whenever feasible, to correct inaccurate information about County Government work (especially on County Government Web sites) that is brought to their attention.
6. County Government employees may not post any personally identifiable information on an SM/W2.0 Web site unless the information would otherwise be released consistent with the Privacy Act and Freedom of Information Act). Questions concerning whether employees may release PII may be directed to the Chief Officer or the operating unit Officer. The improper release of PII or other sensitive information may result civil or criminal penalties, in accordance with the Privacy Act.
7. County Government employees may not improperly use or post materials protected by copyright, trademark, patent, trade secret, data rights, or related protections for intellectual property. Proper use may require obtaining written permission from the owner of such information. The County Government's Office of the Legal Office can assist employees in obtaining these permissions when necessary. Additionally, employees should exercise diligence with respect to the County Government's and their operating unit's intellectual property, in logos, slogans, trademarked names, etc. Employees should not encourage or

allow third-party use of County Governmental emblems or logos without approval, in accordance with, Approval and Use of Seals, Emblems, Insignia and Logos.

8. County Government employees may not include surveys, polls, questionnaires, etc., on official SM/W2.0 Web sites unless the questions have received Clearance from the CO.
9. County Government employees use of SM/W2.0 services should not include requests to contact a member of the county assembly, a jurisdiction, or an official of any Government (National or local) to favour or oppose any legislation, law, or appropriation because these activities are prohibited.
10. County Government Web sites, pages, etc. that contain postings and/or responses by the public require diligent monitoring. Operating units using SM/W2.0 technologies must prevent the posting or immediately delete postings that contain:
 - 10.1 Comments regarding a political party or a candidate in a partisan political campaign (which is a campaign in which candidates are identified by political party);
 - 10.2 Requests to contact a member of county assembly or official of any government, to favour or oppose any legislation, law, or appropriation;
 - 10.3 Advertisements, endorsements, or promotions; and
 - 10.4 Vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups.
11. Because such monitoring and filtering might give rise to public criticism, operating units are required to use either the Office of the Secretary's comment policy or develop and post their own comment policy approved by their Office of Legal Officer.
12. When posting information using SM/W2.0 technologies, agencies should ensure and maximize the quality, objectivity, utility, and integrity of posted information (including statistical information), and ensure that measures are in place to allow for the correction of information not meeting that standard.
13. If the SM/W2.0 technology allows the public to respond to official postings, the County Government Web site must also provide visitors with the ability to communicate with the County Government so that members of the public do not have to register with or provide personal information to third-party Web sites that may require registration or the

provision of personal information. The County Government Web site must provide an alternative way, e.g., e-mail address for members to communicate directly with the County Government without providing personal information to a thirdparty Web site.

14. County Government employees may not solicit consensus advice from the public using SM/W2.0 technologies.

15. Operating units must ensure that the content maintained on their SM/W2.0 sponsors' Web sites, especially PII and other sensitive information, is secure and adequately safeguarded from unauthorized disclosure or destruction. The records must be retained consistent with the County

Government's records retention requirements.

16. Operating units interacting with the public through SM/W2.0 technologies must ensure that such interactions require and generate the least amount of PII possible from their users. To that end, and whenever feasible, operating units must edit and actively manage their SM/W2.0 Web site or application settings to make sure that only the minimum amount of PII necessary to effectively use such technologies is being generated/collected.

17. When visitors to an official County Government Web site are redirected from the County Government site to a third-party site, the visitors must be notified that they are leaving the official agency site, e.g., when a visitor to a

Commerce site is redirected to view a video on YouTube®. Further, County Government employees' use of links to such third-party sites must be consistent with their operating unit's linking policy.

18. The County Government may not rely on SM/Web 2.0 social media as the exclusive means of distribution of information. Materials posted to SM/W2.0 services also must be posted on official Government Web sites, and alternative, non-electronic forms of information must be made available upon request.

19. The County Government does not endorse commercial products or services. County Government employees should not post third-party advertisements or otherwise engage in activities that might lead to a conflict of interest, appearance of endorsement, affiliation, or authorization, or otherwise lead the public to believe that your operating unit supports the views, products, services, etc. of third-parties.

20. County Government Web sites must not collect any personal information from children (under the age of 13) in violation of the Children's Act.

19.4 Applying for Official SM/W2.0 Accounts

County Government employees should consult the list of County Government approved Social Media and Web 2.0 Web sites and apply through the social media manager for SM/W2.0 accounts.

19.5 Specific IT Security Guidelines for Using SM/W2.0 Technologies

SM/W2.0 present IT security challenges beyond those of static Web sites, and it is essential to adhere to applicable County Government IT security requirements, including the following:

- The Administrative Point of Contact (APOC) for a SM/W2.0 account should be solely responsible and accountable for the administration, password control, and access management of the account.
- APOCs should not use the same password for more than one account. Many SM/W2.0 sites allow account administrators to assign administrative rights to other users. When available, this feature should be used instead of sharing passwords.
- Browsing should be performed from non-administrative accounts, and browsers should be configured in a secure manner.
- APOCs must not use the same password for logging in to their Commerce or operating unit network that they use to access any SM/W2.0 site. Failure to use different passwords could compromise the security of the County Government or operating unit network.
- APOCs should only follow links and download files from known and secure sources. Any file downloaded from a SM/W2.0 site must be virus scanned before opening. Upon receipt of a suspicious message, link, or file to download from a known person, APOCs should verify that the item was actually sent by the person before virus scanning and opening it.
- SM/W2.0 accounts must be monitored on a regular basis. In the event pages are hacked or defaced, a report must be sent immediately to Security Incident Team or the operating unit's IT Security Officer. After reporting the incident, the APOC for the account must contact the software or service provider to regain control of the account and restore the page. Passwords will be changed immediately after any hack or page defacement.

CHAPTER TWENTY

20. EMAIL COMMUNICATION

20.1 Definition of Terms

Realtime Blackhole Lists -This a list of IP addresses which are most often used to publish the addresses of computers or networks linked to spamming and most mail servers software can be configured to reject or flag messages which have been sent from a site listed on one or more such list.

Authentication- The process of determining whether someone or something is, in fact, who or what it is declared to be.

SPAM The mass electronic distribution of unsolicited email to individual email accounts.

IMAP It is a protocol for e-mail retrieval and storage

POP3 It is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection

SMTP It is an Internet standard for electronic mail transmission

20.2 Scope

This Chapter of the ICT policy covers email communication at the County Government and applies to all employees, vendors, and agents operating on behalf of the County Government.

20.3 Purpose

The purpose of this email policy is to ensure the proper use of County Government email system and make users aware of what County Government deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within County Government Network.

20.4 Users

The County Government email users will comprise of all County Government employees.

20.5 Statement of Responsibilities

The County Government email users shall be responsible for their own actions. Every user of the email system has a duty shall ensure they practice appropriate and proper use and must understand their responsibilities in this regard. The County Government will ensure that County Government heads of departments and employees are aware of this policy and they will in turn be responsible for informing their stakeholders of this policy. The CO will be responsible for providing and maintaining central email system. The County Government shall oversee the implementation of the email policy.

Staff are required to use only the official email assigned to them for official communication.

All County Government communications including letterheads, posters, envelopes, and such other printed materials must have the official county email printed on them. The use of the email systems such as Yahoo, Gmail, etc is prohibited.

Email messages are regarded in law as having the same status as words on paper; potentially libelous comments must therefore be avoided. Racist, tribal, sexist, xenophobic or otherwise offensive language is unacceptable and could result in the individual responsible and/or the County Government of Nyeri being sued and/or prosecuted.

E-mail should only be used for personal correspondence in accordance with this Policy. You should not invite nor encourage personal e-mail messages to be sent to your official e-mail address, nor should personal emails be sent using your work email address if there is a danger of exposing the County Government to implied contractual commitment or other liability.

You should not disclose your email password to anyone else for any purpose whatsoever.

The County Government of Nyeri reserves the right to monitor the use of e-mail and content. Abuse or misuse of the service may lead to disciplinary action. Defamatory, libelous, abusive, sexist, tribal, homophobic, xenophobic or racist comments in e-mail may render the sender personally liable to civil action.

20.6 Guiding Principles: General Use

20.6.1 The County Government email account should be used primarily for the core functions of the government.

20.6.2 The use of County Government electronic mail for unauthorized commercial activities, personal gain (private or otherwise),

unrelated to the government business, or fundraising is strictly prohibited.

20.6.3 Sending chain letters, press releases, joke emails or other junk-mail of any kind is prohibited.

20.6.4 The use of email must be consistent with County Government applicable policies and practices of ethical conduct and safety.

20.6.5 The use of email to transmit material that infringes the copyright of another person, including intellectual property rights is prohibited.

20.6.6 All government data contained within an email message or an attachment must be secured according to County Government's Data Security, Confidentiality and Privacy guidelines in the ICT policy.

20.6.7 The County Government email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair, colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or tribal or national origin. Email users who receive emails with this content should report the matter to their supervisor or to the Chief Officer immediately.

20.6.8 The County Government email system will not be used for activities that violate the privacy of others or unfairly criticize or misrepresent them.

20.6.9 Creation or transmission of anonymous messages or deliberately forging messages or email header information, without clear identification of the sender is prohibited.

20.6.10 The unauthorized provision of access to County Government services and facilities by third parties is forbidden.

20.6.11 Email that is identified as a County Government business record shall be retained according to appropriate government regulations and .

20.6.12 Users are prohibited from forwarding unauthorized government confidential material through email to a third party email system.

20.6.13 Users are prohibited from using third-party email systems and storage servers to conduct government business, to create or memorialize any binding transactions, or to store or retain email on behalf of County Government unless otherwise authorized by County Government management.

20.6.14 The government does not examine or disclose email content without the user's consent. Nonetheless, subject to the requirements for authorization, notification, and other conditions determined by the management, the County Government may examine or disclose email content where it contravenes the guidelines for general and personal uses stated in this policy are violated. The government may also disclose email content to lawful authorities if and when required through the appropriate legal process.

20.7 Best practices

20.7.1 The County Government of Nyeri considers email as an important means of communication and recognizes the importance of proper email content in conveying a professional image. Users should take the same care in drafting an email as they would for any other communication. Therefore the government wishes users to adhere to the following email guidelines while writing emails:

- a) Write well-structured emails and use short, descriptive subjects.
- b) The County Government of Nyeri's email style is informal. This means that sentences can be short and to the point. You can start your email with '_Hi', or '_Dear', and the name of the person. Messages can be ended with '_Best Regards'. The use of Internet abbreviations and characters such as smileys however, is not encouraged.
- c) Signatures must include your name, job title and name of the department. A disclaimer will be added underneath your signature

(see Disclaimer below)

- d) Users must spell check all mails prior to transmission.
- e) Do not send unnecessary attachments. Compress attachments larger than 5 MB before sending them.
- f) Do not write emails in capitals.
- g) Only mark emails as important if they really are important.

20.8 Personal Use

- 20.8.1** The County Government permits the use of its IT facilities for email by employees and other authorized users for a reasonable level of personal use.
- 20.8.2** Personal communication may be permitted on a limited basis, where the communication is of benefit to the staff and or the County Government.
- 20.8.3** The County Government e-mail communication may not be used in a nature that competes with the County Government in its core functions.

20.9 Quotas and Limits

- 20.9.1** All email accounts have quota limits placed on them. All file partitions are backed up to tape on a regular basis. Accounts that will remain inactive for ninety days will have their files archived according to the preconfigured inbuilt server operations. Unless specifically requested, no archiving will be done for user files after the expiry on the stipulated period.
- 20.9.2** Users will receive email notification when approaching their quota limit and are encouraged to follow server guidelines provided through the notifications to manage their accounts.
- 20.9.3** The final email that fills up the user's quota will always be delivered. Once the quota limit has been surpassed no further email can be delivered to an individual's inbox until they have deleted some emails to create storage space.

20.9.4 Email that fails to be delivered because a user has exceeded his/her quota limit, the email will be held in the local mail queues for four days and the system will retry periodically to deliver. After four days the email will be returned to the sender.

20.9.5 The limit on the size of an email transmitted is 10MB.

20.10 Virus Checking

20.10.1 Messages containing malware will be retained for up to a month for administrative reasons. The sender of such messages will be informed of the viral content of their email. A similar message will be sent to the administrator(s) of the email gateways.

20.11 Logging

Traffic through the County Government email system is logged. Logs include details of the flow of email but not the email content.

Transaction logs are kept online for up to a month. Backups of these logs are kept for up to 3 months. Logs are available to authorized systems personnel for diagnostic and accounting reasons.

20.12 Spam and Junk Mail

Incoming email is checked against other Realtime Blackhole Lists and if successfully matched it shall be marked locally with the insertion of an additional header flag. Email matching the databases will be delivered.

20.13 Remote Access

20.13.1 Remote access to the County Government IMAP email servers is possible via the Internet. Remote access to other POP3/ IMAP mailboxes off campus is permitted via secure methods only.

20.13.2 Access to remote SMTP servers for sending mail is not permitted and is blocked at the firewall. All machines off the campus network are configured to use the County Government's SMTP server, smtp.uasingishu.go.ke for outgoing mail.

20.13.3 Access to the County Government's SMTP servers from outside the workplace is permitted for encrypted and authenticated connection only.

20.14 Incident Handling and Data Protection

20.14.1 The County Government will investigate complaints received from both internal and external sources, about any unacceptable use of email that involves its email system.

Chief Officer will be responsible for the collation of information from a technical perspective. Logs shall be kept for a period of three months, therefore prompt reporting of any incidents which require investigation is recommended.

20.14.2 Where there is evidence of an offence it will be investigated in accordance with the County Government's disciplinary procedures applicable to all members of the County Government. In such cases the County Government will act immediately with the priority of preventing any possible continuation of the incident. Accounts may be closed or emails blocked to prevent further damage or similar incidents occurring.

20.15 Policy Compliance

20.15.1 Compliance Measurement

The County Government will provide an email application form to all employees for email account creation.

The Chief Officer will verify compliance to this policy through various methods, including but not limited to, random log checks, internal audits and feedback to the policy owner.

20.15.2 Non-Compliance

Non-compliance to this policy will be handled by the County Government Disciplinary Committee.

20.15.3 Disclaimer

All mails sent from County Government are subjected to County Government's Email terms and conditions as stated below. These terms should be included in every email sent out from the County Government email system.

"This email and any files transmitted with it are confidential and may be legally privileged and are intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in

error please notify the sender and immediately delete the email from your system.

The County Government of Nyeri disclaims any liability to the fullest extent permissible by law for any consequences that may arise from the contents of any email sent from its systems including but not limited to personal opinions, malicious and/or defamatory information and data/codes that may compromise or damage the integrity of the recipient's information technology systems. Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the County Government of Nyeri."

CHAPTER TWENTY ONE

21. E-WASTE AND DISPOSAL MANAGEMENT

21.1 Definition of Terms

For the purpose of this policy, the following terms refer:

- 21.1.1 E-waste** – old, end-of-life or discarded electrical and electronic equipment and appliances.
- 21.1.2 End-of-life** – end of the useful life of equipment in a particular environment. Also refers to used electronics which are destined for re-use, re-sale, salvage, recycling or disposal.
- 21.1.3 Contractors**- companies or organizations that have entered into business contractual agreements to supply products or services to the County Government
- 21.1.4 Collaborative partners** – these are the organizations, companies, government entities or universities that have entered into an agreement with County Government in a particular field.
- 21.1.5 Community** - a group of individuals, business operators, organizations, partners that interact with the County Government establishment through sharing of resources and establishment of commercial relationships

21.2 Operational Scope of The Policy

This policy caters for Staff, Students, Visitors, community, partners and Contractors across all the County Government Campuses and concerns all electronic equipment (refer to Categories of E-waste below) within the purview of the management.

For the purpose of this policy the following categories of EEE's are possible sources of E- waste:

- a) ICT and Telecommunications
- b) Office Electronics
- c) Large Household and Appliances
- d) Consumer Equipment
- e) Toys, Leisure and Sports Equipment
- f) Lighting
- g) Medical Equipment
- h) Automatic Dispensers
- i) Monitoring & Control Instruments
- j) Batteries
- k) And any other EEE's that may be defined from time to time by Chief Officer.

21.3 Fundamentals of The Policy

The fundamentals and basics that informed this policy is derived from Kenya Government Laws both on the available Legal framework under National Environmental Management Authority (NEMA),

the proper guidelines for E-waste management and the need to establish an advisory committee to handle enforcement and sensitization of this policy including but not limited to information dissemination, resource mobilization and documentations of user manuals.

21.4 Regulatory Environment

Environmental Management and Co-ordination Act, 1999 informs the fundamental basis for this policy.

21.5 Human Resource and Awareness

The Biosafety Committee, ICT shall be the main source of Human Resource to provide capacity in E-waste management Activities. They will assist the County Government develop the following guidelines:

- 21.5.1** Develop a comprehensive E-waste management training toolkit that covers a wide area from technical maintenance, disposal and disassembling, for proper human and environmental safety

21.5.2 Establish proper mechanisms for establishing an Income Generating Unit (IGU) by seeking Public Private Partnerships (PPP).

21.6 Effective E-waste Management Practices on Recycling

This policy shall among other things, ensure the proper utilization of modern technologies that ensure minimalist generation of E-waste, both during recycling process and disposal. This should be within the sound practices that reduce unfavourable environmental and health impacts.

Effective and full proof E-waste management shall be accomplished through the following measures:

- 21.6.1** Recycling should be carried out in designated areas managed in a centralized manner by the County Government.
- 21.6.2** 21.6.2 Effective technologies that maximize recovery and minimize waste generation to ensure safe use of environment.
- 21.6.3** 21.6.3 Recycling Technologies should be modern and cost effective but meet the needs of E-waste handling.
- 21.6.4** 21.6.4 That a proper workforce is Trained and skilled in using environmentally safe operations in handling e-waste.

21.7 Sensitization on E-waste Management and Information Dissemination

The policy underscores the need for effective sensitization to all public and County Government stakeholders on the nature of hazards that E-waste has and therefore, there is need for the County Government to undertake the following:

- 21.7.1** Through Chief Officer and Biosafety Committee chairperson, develop a strategy for training efforts including partnerships with Government/ manufacturers/ retailers/recyclers.
- 21.7.2** Provide all channels to distribute E-waste information including but not limited to Brochures, Posters, Web portal, Manuals and other dissemination tools.
- 21.7.3** Carry out quarterly or annual campaigns to create E-waste awareness through the relevant County Government departments.

21.8 E-waste Resource Mobilization

In its effort to combat the effects of E-waste, the County Government shall provide resources for E-waste management by affecting the following:

- 21.8.1** Create and incrementally raise the budgetary allocation to all departments that carry out E-waste management targeted at reducing E-waste risks.
- 21.8.2** Establish guidelines and roadmap for resource mobilization from development partners both private and public through mutual contracts.

- 21.8.3** Designate or establish buildings, equipment and devices and other support Systems for effective and efficient management of e- waste.

21.9 Implementation of the Policy

21.9.1 E-waste Collection Plan

Generated E-waste within the County Government Processes

The Chief Officer mandated under this ICT Policy shall:

- a) In COLLABORATION with all the Departments and Sections, identify Ewaste in their respective facilities.
- b) In CONJUNCTION with Biosafety Chairperson ensure that E-waste are collected every quarter and kept in an appropriate storage pending the recommendations and approval of Disposal Committee/Biosafety Committee of the County Government .
- c) In PARTNERSHIP with the Biosafety Committee categorize all E-waste generated within the County Government at least once every quarter and prepare a report to the Disposal Committee including recommendations for disposal.
- d) In COLLABORATION with Procurement Office and Biosafety Committee execute the recommendations of the Disposal Committee and prepare a report for the County Government Management.
- e) In COLLABORATION with the office of County Secretary organize quarterly awareness forums for sensitization on E-waste.

21.9.2 Biosafety Committee

The Biosafety Committee shall be the main advisory E-waste committee and is mandated by this policy to:

- a) In conjunction with the Chief Officer oversee implementation of this policy.
- b) Develop procedures and work instructions for collection, sorting, disassembly, packaging, storage and disposal of E-waste.
- c) Through sensitizations and trainings, ensure reduced effects of Ewaste handling
- d) Ensure that all decisions are consistent with the national laws and policies.
- e) Provide flexibility to adopt the changes required from time to time.
- f) Carry our frequent reviews on inputs from all the County Government stakeholders.
- g) In conjunction with the Chief Officer supervise the implementation of this policy and advise County Government management as appropriate.

- h) Advise on review and incremental improvement of this policy from time to time.
- i) In conjunction with the Chief Officer shall develop standards to prevent the importation and donations of useless or harmful E-waste.
- j) In consultation with the Chief Officer shall approve innovative E-waste management technologies that are environmentally sound.

21.9.3 Continuous Research and Development on E-waste

The Governors' Office Department will advise the County Government to carry out specific research on cost effective technologies and effective adaptation of the best available technologies to be adopted by the County Government for E-waste Management.

21.9.4 Staff and Skills

The County Government shall facilitate development of skills requisite for the implementation of E-waste management operations. The staff shall be provided with the requisite instructions and procedures, equipment and devices for E-waste management operations.

21.10 Monitoring, Evaluation and Review Strategies

21.10.1 Monitoring and Evaluation

The Biosafety Committee shall carry out quarterly evaluation and monitoring of E-waste management to ensure compliance with this policy. The output from this policy shall be evaluated, monitored and reviewed from time to time by the Government agencies and any other authorized body.

CHAPTER TWENTY TWO

22. BYOD (BRING YOUR OWN DEVICE)

22.1 Definition

BYOD: Bring Your Own Device, also known as Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP) — refers to the policy of permitting users to bring personally owned mobile devices (laptops, tablets, and smart phones) to the County Government, and to use those devices to access privileged County Government resources (data, information and applications).

22.2 Purpose and Scope

This policy document applies to users accessing County Government network and resources WITHIN or OUTSIDE the County Government using user-owned

devices and works in tandem with County Government ICT policy. County Government has the sole right to amend the policy from time to time when and where it is deemed appropriate. The policy addresses responsibilities and security concerns when using user- owned devices while accessing County Government systems and services.

22.3 Policy Statement

County Government embraces and supports the use of user-owned devices in its network by users. The following stipulate responsibilities where applicable when using user-owned device.

22.4 Device and Support

County Government accepts the following user owned devices on its network; smart phones, tablets, iPads, laptops, Personal Digital Assistant. Any other device outside the listed ones, the user must seek approval from the Chief Officer.

The Governors' Office offers limited support to the user owned devices i.e. configuration for the device to be able to connect the County Government network.

The County Government will also advice the users on the type of e-resources available, how and where they can be accessed from.

22.5 Software Allowed

The users will be required to have installed the acceptable operating system and application software before they are allowed to access the e-resources on the County Government network. The allowed operating systems includes the following; windows, Linux, OS X, android, and mac OS. For the application software the standard applications like browsers and anti-viruses will be acceptable and any other software that will be approved from time to time by the Chief Officer.

The County Government will also advice the users on the software updates and upgrades for them to be able to use their devices efficiently.

22.6 User Obligations and County Government Disclaimers

22.6.1 Obligations for the Users

The users have the following obligations to adhere to;

1. Familiarizing themselves with their devices and security features to ensure safety of County Government data/information.
2. Protecting sensitive information such as medical information of students and staff
3. Destroying or returning all data belonging to County Government once they are no longer authorized or owner of the device(s).
4. Users will not store sensitive data/information in their devices without authority of their immediate supervisors.
5. Installing, upgrading the software and installing patches to their device so as to improve security of County Government information and/data.
6. Removing any County Government information/ data when finished and not storing or sending any copies without authority.
7. Being responsible of the consequences caused by software and hardware installed on their own devices.
8. Keeping information/data safe and confidential.
9. Conducting themselves responsibly so as not to disrupt normal County Government functions
10. Taking care of their own devices and using them in a right way i.e not using own devices to violate institution or other users rights, also not using own devices to access restricted content like porn.
11. Were to and comply with BYOD policy

22.6.2 Disclaimers:

- a) Shall NOT take responsibility for maintenance, damage, theft or loss of user-owned devices, data or software
- b) Does NOT take responsibility for failure of user-owned devices to operate normally.

22.6.3 Monitoring of User-Owned Devices

The County Government reserves the right to prevent access to content that it might deem as harmful or unauthorized in the network.

In exceptional circumstances, the County Government will be required to access its data being stored on the user-owned devices, but personal privacy will not be violated.

The County Government data and information will only be stored and processed on user-owned devices upon approval by the section head. However it can be deleted, amended or retrieved for the user-owned device by the Chief Officer.

Some users on specific networks will be blocked from accessing certain websites during work hours (8am to 5pm, Monday to Friday) while connected to the County Government network. Such websites include, but are not limited to Facebook and YouTube as it will be determined from time to time by the Chief Officer and the users will be notified.

22.7 Security of Systems

The County Government is investing in making sure that there are proper security measures that protect the data/information available on the County Government network. The users will be required to comply with all security measures that will be put in place.

The users will be responsible for protecting intellectual property right where information and data is not supposed to be for public consumption.

The users will also be tasked to maintain the integrity of the data / information contained on their devices.

In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the County Government network.

The County Government Chief Security Officer will be checking/proving ownership of all devices where necessary. Also he / she will take necessary actions following any suspicions of theft or security risk to County Government resources. The County Government will refuse, restrict or withdraw access to user where necessary i.e. where the user violates whatever is stated in this policy.

22.8 Incidents and Reporting

The users will be required to report the theft of their own devices to the chief security officer within 24 hours. Also, in case of security breaches to the ICT infrastructure the user will be required to report to the Chief Officer within 24 hours.

CHAPTER TWENTY THREE

23. INFORMATION SECURITY

23.1 Introduction

The County Government of Nyeri recognises that ICT systems and information are valuable assets which are essential in supporting the County Government's strategic objectives. The County Government recognises its obligations to protect information from internal and external threats and recognises that effective information security management is critical in order to ensure the successful enablement of ICT and delivery of business functions and services. The County Government is committed to preserving the confidentiality, integrity and availability of all physical and electronic assets.

Information security management is an ongoing cycle of activity aimed at continuous improvement in response to emerging and changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorised access, disclosure, modification or destruction and is vital for the protection of information and the County Government's reputation.

This policy details the County Government of Nyeri's approach to Information and Communications Technology (ICT) Security Management and contains no sensitive or restricted information and may be freely publicised to relevant parties. A current version of this document is available to County Government staff on the County Government's intranet and is available to external parties on the County Government's website at www.nyeri.go.ke.

The approach is based upon recommendations contained within ISO27002 code of practice for information security management.

23.2 Scope

This ICT Security Policy applies to:

- a) ICT systems belonging to, or under the control of, County Government of Nyeri;
- b) Information stored, or in use, on County Government ICT systems;

- c) Information in transit across the County Government's voice or data networks;
- d) Control of information leaving the County Government;
- e) Information access resources;
- f) All parties who have access to, or use of ICT systems and information belonging to, or under the control of, County Government of Nyeri including:
 - i. County Government employees
 - ii. Contractors
 - iii. Temporary staff
 - iv. Students on attachment or internship
 - v. Partner organisations
 - vi. Members of the public
 - vii. Volunteers
 - viii. Consultants
 - ix. Any other party utilising County Government ICT resources

Application of this policy applies throughout the information lifecycle from acquisition / creation, through to utilisation, storage and disposal.

23.3 Responsibilities

23.3.1 Co-ordination: The County Government co-ordinates information security management across the organization through an internal Information Governance framework within the Directorate of ICT .

23.3.2 Security Officer: The County Government's Information Security Manager is responsible for ensuring policies and procedures are in place to cover all aspects of ICT systems and Information security. All policies will be communicated across The Directorate of ICT to ensure good working practices and to minimise the risk to the County Government's reputation.

23.3.3 Heads of Departments: are responsible for ensuring that ICT systems and information within their service areas are managed in accordance with the County Government's ICT Security Policy. Day to day responsibility for the management of ICT systems and information may be delegated to staff designated as information or system owners within departments.

23.3.4 Users of Resources: It is the responsibility of any individual or organisation having access to the County Government's ICT systems and information to comply with the County Government's ICT Security Policy, associated guidelines and procedures and to take adequate steps to safeguard the security of the ICT systems and information to which they have access. Any suspected or actual security weakness, threats, events or incidents must be immediately reported to the Chief Officer responsible for Governors' Office via the County Government's Incident Reporting system

23.4 Policy Statement

The Information Security Policy is based on the principles set out in the British Standard for Information Security - *ISO/IEC 27002*

The County Government is committed to the development and maintenance of an Information Security Management System based upon the International Standard the County Government has developed this ICT Security Policy to:

- a) Provide direction and support for ICT security in accordance with business requirements, regulations and legal requirements;
- b) State the responsibilities of staff, partners, contractors and any other individual or organisation having access to the County Government's ICT systems;
- c) State management intent to support the goals and principles of security in line with business strategy and objectives.
- d) Provide a framework by which the confidentiality, integrity and availability of ICT resources can be maintained.
- e) Optimise the management of risks, by preventing and minimising the impact of ICT security incidents;
- f) Ensure that all breaches of ICT security are reported, investigated and appropriate action taken where required;
- g) Ensure that supporting ICT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats;
- h) Ensure ICT information security requirements are regularly communicated to all relevant parties.

23.5 Authorised Use

Access to ICT systems and Information for which the County Government is responsible is permitted in support of the County Government's areas of business or in connection with a service utilised by the County Government. Authorised users are defined as: County Government employees, authorised contractors, temporary staff, partner organisations or members of the public when using public information services provided by the County Government.

23.6 Acceptable use

All users of ICT systems and information for which the County Government is responsible must agree to, and abide by, the terms of the County Government's Acceptable Use Policy, associated security policies and applicable Codes of Connection or Conduct.

23.7 Security Awareness

The County Government is committed to promoting safe working practices. All employees will receive security awareness training commensurate with the classification of information and systems to which they have access. Staff working in specialized roles will receive appropriate training relevant to their role. Relevant information security policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees' responsibility to ensure they are adequately informed of information security policies and procedures.

23.8 Business Continuity

The County Government has developed, and maintains, a Business Continuity Strategy (need to develop a comprehensive strategy) based on specific risk assessment to maintain critical business functions in the event of any significant disruption to services or facilities on which the County Government is reliant.

23.9 Monitoring and Reporting

The County Government reserves the right to monitor the use of ICT systems and information, including email and internet usage, to protect the confidentiality, integrity and availability of the County Government's information assets and ensure compliance with the County Government's policies. The County Government may, at its discretion, or where required by law, report security incidents to the relevant authorities for further investigation. As part of the standard audit review process, Internal Audit will routinely assess compliance with the county's ICT Security Policy and applicable ISO27001 controls and report matters to senior management or the Information Governance Group where appropriate. Security incidents reported through the Security Incident

Management Policy and Procedures, will inform on the effectiveness of ISO27001 controls and assist in identifying training and awareness requirements and improvements through the Corrective and Preventative Action (CAPA) procedure.

23.10 Risk Assessment

The County Government has developed a Risk Management Strategy and the risk to the County Government's ICT systems and information will be managed under this framework with reference to the guidelines detailed in *BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management*. Reviews are independent, unbiased and verified by either internal audit or external parties when required.

23.11 Security Policy Review

The County Government will conduct an annual review of the policy or following any significant security incidents, changes to the county's legislation or changes to the County Government's business requirement or structure.

23.12 Asset Management

The County Government will maintain an inventory consisting of all information assets which will be managed in accordance with the County Government's information security policies and procedures.

23.13 Sanctions

Failure of County Government employees to comply with the County Government's Information Security Policy may lead to disciplinary action under the County Government's disciplinary procedure.

Failure of contractors, temporary staff, public, partners or third party organisations to comply with the County Government's Information Security Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

23.14 Development of specific ICT policies, procedures and guidelines

The County Government of Nyeri is committed to the ongoing development and review of ICT policies, procedures and guidelines to manage the risk of emerging threats to its systems and services. This work will be coordinated by the Information Governance Group chaired by the County Secretary. A list of current supporting documents is included in Appendices New policies,

procedures and guidelines are distributed to all stakeholders at the time of issue. Appendices of this policy are updated during the annual ICT Security review.

CHAPTER TWENTY FOUR

SOFTWARE AND APPLICATIONS

INTRODUCTION

This Section describes standards for developing (or purchasing and installing) and maintaining/managing computer applications for administrative purposes in the County Government. The degree to which the responsibility for development, implementation and maintenance of systems is centralized in a single administrative ICT department versus decentralized and handled by the functional offices varies. While these documents will sometimes refer to the "ICT department", these standards apply to any department or any vendor engaged by the County Government that undertakes development, installation or maintenance of ICT applications. The determination for when these standards apply depends on the nature of the application, not on who is responsible for the development.

There are two main characteristics of applications which must be considered when determining

how these standards apply:

1. The size and complexity of the application; and
2. Some measurement of how essential the system is to the operation of the Department or the County Government as a whole, and therefore how much risk is associated with whether or not the development efforts are successful.

A system should be considered high risk if a failure of the system to function correctly and on schedule could result in a major failure by the County Government to perform essential functions, a significant loss of funds to the County Government, or a significant liability or legal exposure to the County Government.

Policy Objectives

- a) The purpose of this policy is to ensure that the process of software development at the ICTC follows the due process right from the planning phase through to the implementation stage and that all deliverables at every milestone meet the required standards.
- b) This policy also seeks to continually improve on the process of software development at the ICTC and ensure that the software products produced meet the requirements of the user and are of good quality.
- c) This policy also addresses the need for software support and use of the available information to ensure that the integrity of the system is not compromised at any time. The need for ownership of software by users is also addressed to apportion responsibility and improve access to this information.

Scope

Overview This document establishes a common framework for software life cycle processes, with well-defined terminology, that can be referenced within the County

Government. The document applies to the acquisition, supply, development, operation, maintenance, and disposal (whether performed internally or externally to the County Government) of software systems, products and services, and the software portion of any system, Software includes the software portion of firmware.

Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this policy. All standards are subject to revision and, since any reference to a standard is deemed to be a reference to the latest edition of that standard, parties to agreements based on this standard are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below.

Systems and Applications Standard Second Edition 2019 ICTA.6.002:2019

Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards

- ISO/IEC 12207:2017 Systems and Software Engineering - Software lifecycle processes
- ISO 90003:2018 Software engineering Guidelines

Software Development Policy Statements

The Systems Administration section within ICT Department is responsible for developing, and maintaining County wide systems. In order to provide a standard and reliable support to the County citizenry, Directorate of ICT has come up with a flexible policy, which will govern system development & support in the County Government of Nyeri.

External ICT Departments:

System Development section shall provide systems development and support for County wide applications. However:

- a) Departments & Directorates may be allowed to buy software or customize software limited to internal usage.
- b) Departments & Directorates planning to buy software will need to acquire pre-approval for purchase from Directorate of ICT. Directorate of ICT will need to verify if the County already has licenses for the software requested or not. In addition, Directorate of ICT will verify if proposed software is compatible and conforms to County standard development software/operating systems.
- c) System Development Section shall not provide any support to any systems built outside of ICT Department. System Development Section will not accept to inherit any systems developed outside of ICT Department or purchased without approval from ICT Department.

Project Planning & Organization

- a) Prior to the computerization or acquisition of any County information system, the Director, ICT in consultation with the relevant authority shall constitute an IS project team comprising all the relevant stakeholders.
- b) The Chief Officer in charge of ICT shall appoint a Project Leader for every project.
- c) In case the Project Leader finds that there are some stakeholders that have been excluded from the project team then he or she shall make a request to the Chief Officer for them to be included.
- d) The DBA shall be part of the project team and shall be responsible for advising the team and implementing issues relating to the database management and administration.
- e) The Director, ICT shall ensure that each IS Project has an organization chart.
- f) The roles and responsibilities of the different persons involved in the project development and implementation shall be clearly defined.

Requirements Phase

- a) In this phase of software development, the Systems Analyst shall identify all business, functional, constraint and quality (including performance, compatibility, usability and security) requirements of the envisaged system in consultation with the Stakeholders of the system.
- b) In this phase, the Project Leader shall review the efficiency of the business processes to be computerized through re-engineering. Any recommendations that come out of the re-engineering process shall be communicated to the main stakeholder and Director, ICT who shall be responsible in for channeling them to the relevant County organs for adoption in the County.
- c) At the end of the requirements phase, the Project Leader will present to the stakeholders a requirement specification document. The stakeholders will then validate the document to verify that their requirements have been captured correctly in accordance with the documentation standards
- d) The system users shall have reasonable time to review requirements and sign the user requirement specification document to indicate concurrence with the recorded specifications. Consequently, the requirements shall remain frozen until the system is implemented and deployed to the user department. In the event that certain unforeseen specifications or due to an adverse effect the specifications require to be revised, the entire process of system development will be restarted.

Design Phase

The design phase shall have the following sub-phases:

- a) Preliminary design phase - In this phase, the Systems Analyst in conjunction with the Project Leader and the Documentarist shall produce a design document showing the overall design of the new system. The deliverables in this phase shall be a design document.
- b) Main design phase - In this phase, the Systems Analyst in conjunction with the Project Leader and the Documentarist shall perform detailed design of the functionality of the new system with the aim of establishing complete details of all the possible actions and results in the requirements This phase shall cover input/output design and a logical data model of the envisaged system. The

deliverable in this phase shall be a Design or Functional Specification document and the User Interface Design.

- c) Review or Validation Phase: in this phase, the Project Leader in consultation with the Stakeholders shall review and validate the design documents and make any changes as recommended or appropriate. The result of this phase shall be validated design documents.

Monitoring and Evaluation

- a) The Project Leader shall put in place modalities for ensuring that the system developed is reviewed after every six months or such a time deemed fit to find out if the System is still fulfilling the user requirements, and if not, appropriate actions taken to ensure that the System meets the ever-changing user needs.
- b) A system that is too costly to maintain, does not meet user requirements or is deemed to be obsolete shall be retired after consultation with all stakeholders.

MIS Support and Use

Technical Support

The Manager, ICT shall ensure that every project has alternatives for staff that provide essential support service to guarantee that services are provided even in the absence these staff members. This is important for the continuity of systems and the avoidance of over dependence on one staff member whose absence can disrupt user services.

User Requests

All user requests for data or service by the users or stakeholders of any MIS system shall be channeled through the Director, ICT or such other approved communication channel.

Response to Requests

This shall be done as per the ICT Department service charter

Data Collection and Updates

All users shall be responsible for collecting, updating, validating and verifying all data required by all Information Systems in their custody. In exceptional cases of emergency or data migration, ICTC staff may be called upon to offer support, in such cases the system data owner shall validate the migrated data within a reasonable time and in any event not exceeding three months.

Tracing Data Update

Transactions shall be made traceable through the system by use of audit trails.

Project Team for Each System

- a) For each MIS project, there shall be an ICT Project Team whose composition shall be determined by the Deputy Manager (MIS).
- b) There shall be functional meetings for each MIS regularly at least one every quarter.

System Ownership

The Directorate of ICT shall be the Custodian of all software within the County Government of Nyeri if the user department wishes to take ownership of the system they shall be responsible for the daily operation of the system and shall appoint a System Administrator who must meet the minimum requirements for the position of System Administrator.

Accessibility to Information Systems

This is done as per the ICT Department service charter.

CHAPTER TWENTY FIVE

24. BREACHES OF POLICY

24.1 Network Security

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government assets, or an event which is in breach of the County Government's security procedures and policies.

All County Government employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organization contracted to support or access the Information Systems of the County Government.

The County Government will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

24.2 Wireless Access

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government assets, or an event which is in breach of the County Government's security procedures and policies.

All employees, interns, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organization contracted to support or access the Information Systems of the County Government.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the County Government's ICT systems or network results from the non-compliance, the County Government will consider legal action against the third party. The County Government will take appropriate measures to remedy

any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the County Government's disciplinary process.

24.3 Access Control

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government of Nyeri assets, or an event which is in breach of the County Government's security procedures and policies.

All County Government employees, interns, students on attachment, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the County Government.

The County Government will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the disciplinary procedures.

24.4 Server Security

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government assets, or an event which is in breach of the County Government's security procedures and policies.

All County Government employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the County Government.

The County Government will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant

frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

24.5 Public Internet Access

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Public or County Government assets, or an event which is in breach of the County Government's security procedures and policies

All employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the County Government. In the case of inappropriate use by a member of the public then access rights to the public internet facility may be temporarily suspended or permanently removed dependent upon the level of breach that has occurred. In all instances, where potential criminal activity is suspected\reported the matter will be reported to the Police.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the County Government's ICT systems or network results from the non-compliance, the County Government will consider legal action against the third party. The County Government will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the County Government's disciplinary process.

24.6 Third Party Connection

Breaches of Third Party Connection agreements and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government assets, or an event which is in breach of the County Government's security procedures and policies.

The County Government will take appropriate measures to remedy any breach of a third party connection agreement. If a breach/security incident relates to a Third Party the County Government reserves the right to immediately terminate the Third Party connection and, subject to the nature of the breach/security incident, seek compensation or take legal action. If it

can be determined that the breach/security incident has been caused by an employee of the third party, the County Government would retain the right to request the employer to remove their employee from County Government premises.

If the breach/security incident is determined to have been caused by an individual employed by the County Government, the matter may be dealt with under the disciplinary process

24.7 ICT Asset Management

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government assets, or an event which is in breach of the County Government's security procedures and policies.

All employees, interns, students on attachment, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the County

Government

The County Government will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

24.8 Server Security

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government assets, or an event which is in breach of the County Government's security procedures and policies.

All County Government employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organization contracted to support or access the Information Systems of the County Government.

The County Government will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

24.9 Encryption

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to County Government assets, or an event which is in breach of the County Government's security procedures and policies.

All County Government employees, elected members, volunteers, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the County Government's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the County Government.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the County Government's ICT systems or network results from the non-compliance, the County Government will consider legal action against the third party. The County Government will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the County Government's disciplinary process.

**NB: For the rest of the Chapters of this Policy, any breaches will be interpreted according to the above policy directions
This document forms part of the County Government's ISMS Policy and as such, must be fully complied with.**

LIST OF THE CONTRIBUTORS

No.	Name	Designation
1.	H.E. Hon. Mutahi Kahiga	Governor
2.	Mr. Benjamin Gachichio	County Secretary
3.	Njeru Beth Karimi	CEC Member County Public Service and Solid Waste Management
4.	Kendi Tarichia	CEC Member for Trade, Tourism
5.	Macharia Margaret Wangechi	CEC Member for Education, Culture & Social Services
6.	Dr Rachael Kamau	CEC Member for Health Services
7.	Kinyua Fredrick Wanjohi	CEC Member for Environment, Energy & Natural Resources
8.	James Wachihhi	CEC Member for Agriculture
9.	Kariuki Muthui	CEC Member for Roads and Infrastructure
10.	Dr. Wanjaria Daniel Kwai	CEC Member for Land and Housing
11.	Mwangi Robert Thuo	CEC Member for Finance & Economic Planning
12.	Ruth Mwangi	Chief Officer for Agriculture
13.	Simon Wachira Ngatia	Chief Officer – Education, Culture & Social Services
14.	Newton Wambugu	Chief Officer – Health Services
15.	Pauline Ndegwa	Chief Officer – Environment
16.	Ibrahim Adan Eden	Chief Officer – Trade & Enterprise Development
17.	Joseph Kanyi King'ori	Chief Officer for Public Service Management
18.	Hannah Maranga	Chief Officer – Lands & Housing
19.	Julius Ringera	Chief Officer – Roads, Transport & Infrastructure
20.	John Ngugi	Chief Officer – Finance & Accounting
21.	Francis M. Kirira	Chief Officer –Economic Planning
22.	Dadson Ngatia	Ag. Head – ICT
23.	Charles Mugambi	ICT Officer – Networks and Hardware Support
23.	Abednego Nganga	ICT Officer – Systems Development & Support
24.	Valentine Wanjiru	ICT Officer – Systems Support
25.	Derrick Kiragu	ICT Officer- User Support

REFERENCES

1. E-Government Strategy 2011-2014. *Directorate of e-Government*, February 2011.

2. National Information & Communications Technology (ICT) Policy, *Ministry of Information & Communications*. January, 2006.
3. ISO 9126-1 Software Product Quality, ISO/IEC 9126-2 on External usability metrics, ISO/IEC 9126-3 on Internal usability metrics, ISO/IEC 9126-4 on Quality in use Metrics, ISO 9241-11 Guidance on usability, ISO 14598 – 1 on Software product evaluation, ISO 27799 – Information security management in health using ISO/IES 27002
4. ICT Standards and Guidelines, *Directorate of e-Government - Kenya*, March 2011
5. **ISO** 27001-2 Standards for Security Management and Information Security
6. ISO/TS 29585:2010 Health Informatics standards
7. Standards and Guidelines for Electronic Medical Record Systems in Kenya. *Ministry of Medical Services and Ministry of Public Health & Sanitation*. September, 2011.