REPUBLIC OF KENYA

COUNTY GOVERNMENT OF BOMET

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

P.O. Box 19 – 20400
BOMET
Email: info@bomet.go.ke
Website: www.bomet.go.ke

OCTOBER 2014

VISION

To be a leading and prosperous county with a high level of efficiency and effectiveness in the management of county socio-economic development processes to maximize on resources and achieve high quality of life for the people

MISSION

To foster sustainable socio-economic development through correct Development, interpretation, dissemination and implementation of county development plans and policies, mobilization of resources, effective planning, coordination and participatory selection of community projects

Foreword

The use of Information and Communication Technology (ICT) is very vital in enabling County Government towards achieving its vision.

The purpose of this ICT Policy is to establish a framework for implementing extensive security and control over the use of computerised information systems and equipment in the County.

Dependency on the information technology to provide effective operation of the business and service delivery in modern world is a necessity. It is essential, therefore, that the ICT infrastructure and Systems be secured from destruction, corruption, unauthorised access and breach of confidentiality whether accidental or deliberate.

All forms of information need to be protected, regardless of the medium (e.g. paper, diskettes, USB disks, computers, networks, and telecommunications) used for communication or storage. All County Government's employees and contractors are responsible for protecting the organisations information. To accomplish this, this document will establish proper safeguards to protect information from accidental or intentional unauthorised modification, destruction, and disclosure.

This document establishes base policies, standards and guidelines to protect County Government's information assets stored on its distributed computing platforms, and provide a framework for the continued development of these rules as the processing environment changes.

David Kipyegon Cheruiyot
Executive Member – Finance, ICT and Economic Planning
County Government of Bomet

Preamble

Information and Communication Technology (ICT) has become the backbone of day to day operations in all organizations, County Government of Bomet is not an exception. This ICT Policy document therefore seeks to provide guidelines for compliance, acceptable and secure use of information communication technology by CG employees, County's business partners, customers plus all other stakeholders. This policy further aims to define governance and management structure for the development and implementation of ICT strategies and services; and define the role of the County's Information and Communication Technology Unit.

It is worth noting that all County's ICT facilities and information resources remain the property of County Government of Bomet and not of particular individuals, teams or departments. It is in view of this fact that this ICT policy aims to enhance information security of CG systems, efficient use of information systems by county employees and the affiliates, availability of ICT systems, boost spirit of awareness, co-operation, trust and consideration for others in addition to enhancing compliance with the laws of Kenya. It also provides governance framework for the County's ICT services in relation to best standards.

This ICT policy document relates to all Information Technology facilities and services provided by the County including email system, databases, ERP (Enterprise Resource Planning), operating systems (windows), internet, telephone systems, wireless communication, printers and copiers, just to mention a few. All CG employees as well as business partners are expected to adhere to it.

Charles Cheruiyot Koech
ICT Director
County Government of Bomet

Table of Contents

List of abbreviations and Acronyms

Abbreviation	Description
CG	County Government
BCM	Business Continuity Management
BCP	Business Continuity Plan
DE	Does not Exist
ERP	Enterprise Resource Planning
FE	Fully Exists
GOK	Government of Kenya
GPS	Geographic Positioning System
ICT	Information and Communication Technology
IPSec	Internet protocol security
IT	Information Technology
KM	Knowledge Management
MTP	Medium Term Plan
PE	Partially exists
SAN	Storage Area Network
SLA	Service Level Agreements
SSH	Secure Shell
TCP	Transmission Control Protocol
VLAN	Virtual LAN
COBIT	Control Objectives for Information and Related Technologies
ITIL	Information Technology Infrastructure Library
ITGI	Information Technology Governance Institute

HOD	Head of Department
CRF	Change Request Form
PC	Personal Computer
IPSec	Internet Protocol security
VPN	Virtual Private Network
USB	Universal Serial Bus
DVDs	Digital Versatile Discs
FTP	File Transfer Protocol.
IM	Instant Messaging
MAC	Media Access Control address
IA	Internal Audit

1. Introduction

The Government of Kenya is committed to implement initiatives that will lead to the full achievement of e-Government. The actions will be operationalized in the short term, medium term and long term based on improving communication within government, between government and business and between government and citizen.

To that end, the department of Finance, ICT and Economic Planning (ICT Division) has developed an ICT Policy that will be used to guide the information technology investments within the county as it seeks to align itself to the e-government initiatives. The County Government Integrated Development Plan 2013-17 sets out a clear strategy of how the county will work towards achieving positive results to benefit all Kenyans. It is expected that this will be achieved by working in partnership with all and stakeholders. For this to happen, the County Government needs to strengthen its information technology capacity to support its development plan. This will be achieved through the consistent implementation of the ICT policies outlined in this document.

These Policies establish institutional guidelines that will integrate the use of ICT into the county operations for effective service delivery. This policies, together with the accompanying ICT Strategy and structure will address the need to transform the county into a more effective and efficient government through information and knowledge sharing and process automation.

ICT Unit will be housed and guided by the County Executive Committee Member in charge of Finance, ICT and Economic Planning.

1.1.1 Purpose of the ICT Policy

This policy aims to define a governance and management structure for the development and implementation of ICT policies, strategies and services; and define the role of the county's Information and Communication Technology Unit.

It provides governance framework for the county's ICT services in relation to best standards.

The Guiding principles

These Policies are supported by a set of common practices and Information Technology Standards highlighted below;

ISO 17799-2005 - establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management.

Control Objectives for Information and Related Technologies (COBIT) - an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

Information Technology Infrastructure Library (ITIL) - a widely adopted guidance for IT service management worldwide. It is non-proprietary best practice that can be adapted for use in all business and organizational environments.

IT Governance Institute (ITGI) standards - The ITGI was established in recognition of the increasing criticality of information technology to enterprise success. ITGI conducts research on global practices and perceptions of governance of IT for the business community. ITGI aims to help enterprise leaders understand how effective governance can make IT successful in supporting the enterprise's mission and goals.

These policies have been categorized into the following nine Information Technology Components;

IT Governance

Information Technology Security

IT Risk Management

Privacy and Data Protection

IT Physical and Environmental Management

Change Management

Asset Management

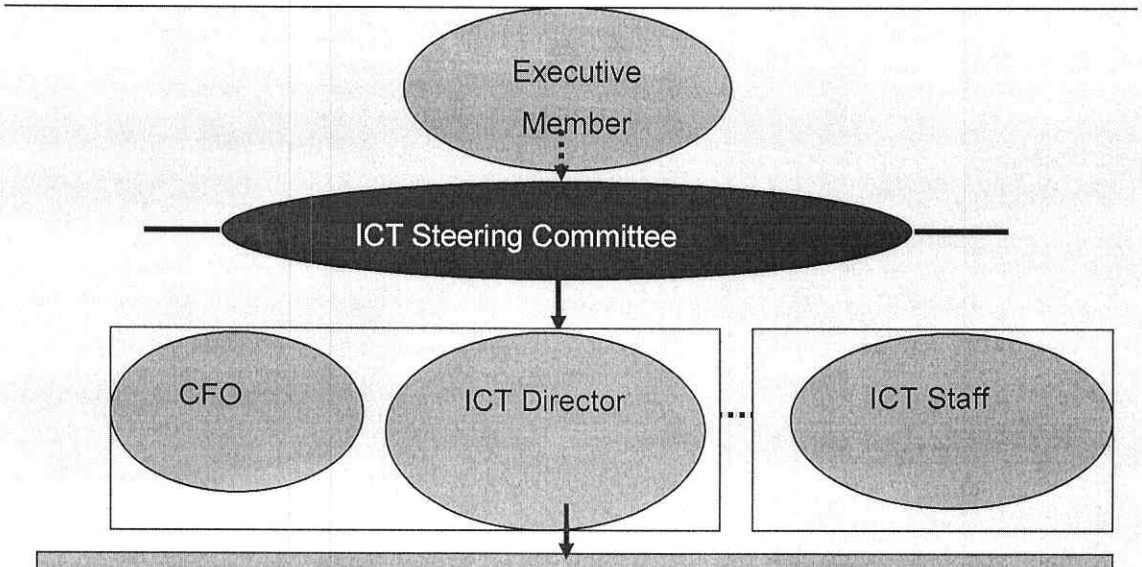
Business Continuity Management

Incident Management

2. IT Governance

The County Government IT governance structure establishes the strategic, operational, and technical decision-making process required to ensure IT enables the county to excel in its mission. IT governance provides strategic leadership, establishes county-wide IT priorities and policies, and is accountable and transparent to the community. The following diagram illustrates the committee structure for IT governance at the county

Structure of County Government's ICT Governance



Issues addressed:

The relevance of latest developments in IT from a corporate perspective

The achievement of strategic IT objectives and alignment of IT with the County Government direction

The availability of suitable IT resources, skills and infrastructure to meet strategic objectives

The role and the value delivery of external IT sourcing

IT Risk management and aspects of IT investments and optimisation of IT costs

Major IT projects

The contribution of IT to the business especially delivering the county mandate

Exposure and containment of IT risks, including compliance risks

3. Information Technology Security Policies

Introduction

Computer information systems and networks are an integral part of operations at County Government thus the organization has made investment in human and financial resources to source and implement these systems. These policies and directives have been established in order to:

- Implement identified IT strategies
- Protect ICT investment
- Safeguard the information contained within these system; and
- Protect the reputation of county government

Password Policy

All user-level passwords (e.g., application user, email, web, desktop computer, etc.) shall be changed from time to time and be at least 8 characters long. Passwords shall be changed immediately if they become, or are suspected of having become compromised.

A password shall not be the same as any of the previous three passwords used for the same account.

Passwords shall require a combination of at least three of the following characteristics: alpha, numeric, upper and lower case, or special characters.

Initial passwords for all new user accounts, or reset passwords assigned when the user has forgotten the password, shall be given to users in a secure manner. The use of third parties or unprotected (clear text) electronic messages shall not be used. Initial or reset passwords shall only be valid for the first log-on and thereafter users shall be required to change the password.

System and Security Administrator passwords (e.g., root, enable, Administrator, System) shall be a minimum of twelve characters long.

System and security administrative passwords shall be changed immediately whenever there is a change in administrative responsibility.

Passwords shall not be identifiable with the user (such as first name, last name, spouse name friends, relations, colleagues, or other easily guessed names).

The User ID shall be locked and users prevented access to the network after a maximum of 3 consecutive invalid login attempts for that User ID.

The User IDs for users with privileges such as root, administrator or supervisor shall never be suspended as their suspension could create a denial of an essential service. In lieu of suspension for such accounts, there shall be a time delay that increases with each invalid attempt, so as to make brute force guessing attacks infeasible.

Default vendor passwords shall be immediately altered following installation of systems or software.

User Account Administration

All County Government Employees shall notify their supervisors when there is any change in their user account (i.e., access to an additional system required, system access no longer required, higher/lower level in access is required).

Human Resource Management shall:

Inform IT department in advance about new recruits, staff transfers, redeployment or termination of employment contracts.

Hand over the HR Reference Manual to new staff which will include detailed security policies and a compliance agreement form.

Head of departments Management shall:

Notify ICT office whenever they become aware of a change in the status of one of its users.

Approve all changes in user accounts.

Continually evaluate user privileges on the basis of need to know and least privilege.

Approve and monitor the access of users to data for which they are responsible.

ICT office shall administer user accounts in accordance with this policy and standards.

General User Identification and Security Guidelines

In addition to the general Application and System Security Minimum Baseline Standards, the following policies will be affected:

Approval of User ID Issuance: The information owner will approve user IDs based on a documented need and job function.

Notification of User Job / Function Changes: Supervisors and HODs must notify the IT department of changes in the employee's job function in order to ensure that access privileges are appropriately adjusted.

Notification of Extended User Absences: Supervisors and Managers will formally notify the IT department of extended absences (e.g., long-term sick leave, temporary transfers, etc.) in order to ensure that computer access is temporarily revoked.

User ID Expiration Dates for Non-Employees: For contract employees and consultants, an ID expiration date that coincides with the conclusion of the contracted project will be created.

Privileged Accounts: Users granted privileged access (i.e. access to system security mechanisms, etc.) will use a different account name than that of normal user.

Auditing User Accounts: On a quarterly basis, information security and system administrators will conduct an audit of current user accounts to ensure that the accounts of unauthorized users have been removed.

Application Access Restrictions: Access to county government application resources will be restricted to authorized users. All access to application system resources will be protected by assigning individual user rights.

Authorization Based on Need: Authorization to modify data or execute commands, transactions or programs, or other access to production data will be defined on a need-to-know basis by job function.

Written Requests for Access Changes Required: To obtain or change access privileges, a representative of the user department should complete and sign a change request form (CRF) that requests the specific access privileges and submit the documentation to the IT department. The IT department will then submit the form to the appropriate application owner who will approve or deny the request. The system administrator will then make the necessary changes to the access privileges for approved requests.

Segregation of Duties: Appropriate segregation of duties related to application systems will be maintained.

Control Access to Application Security Tables: Application-level access control tables and profiles (the lists maintained within a computer application that contain access authorizations) will be protected from unauthorized access. Generally, the system administrators should be the only people with access to these functions.

System Isolation: Extremely sensitive application systems will be run on dedicated and isolated processors.

Transferred or Terminated Users

Notification of User Termination/Transfer: HODs, Supervisors and the Human Resource Department will notify the IT department immediately upon the resignation, termination or transfer of employees to ensure that their access to corporate systems is revoked.

Revocation of User Credentials: All IDs and passwords will be revoked upon termination/resignation of employees and revoke/modify access upon transfer of responsibilities.

Supervisor Coordination with System Administrator: For situations where users with access to highly sensitive information are terminated, the employee's supervisor is responsible for directly coordinating with the

system administrator or other appropriate supervisor to remove the user's access rights.

User Clearance Requirements: All PCs, Phones, Modems, keys, ID cards, software, data, documentation, manuals etc. of terminated personnel must be returned to the employee's direct supervisor or the Human Resource Department, as appropriate.

Antivirus Policy

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of IT resources.

Virus detection software/ Antivirus shall be installed on all servers, laptops and desktop computers and shall be updated continuously with the latest updates available. The antivirus should be updated at least once a week.

Files on any media (removable storage media/fixed storage media) from third- party sources shall be checked / Scanned with the anti-virus program before copying the files into any County Government system.

Users shall be prohibited from writing, compiling, copying, distributing, executing or attempting to introduce any program code that may damage, hinder performance and/or change a computer system or network setting.

Any program code that a user deliberately, accidentally or mistakenly distributes through any means, without the approval of the ICT shall be considered a threat to County Government's information system.

Users, including outsourced personnel, contractors, and consultants shall not install any software or hardware used to circumvent County Government's information security policies. These might include password hacking tools, decrypting tools, discovery tools, and the like. These software and hardware shall be held under strict control, and only loaded when necessary.

County Government staff suspecting a virus infection in any of county's computer system shall immediately report to Information Technology staff members for immediate attention and disinfections.

ICT section to install and maintain up to date corporate antivirus system with centralised administration kit

Firewall Policy

All external and wireless connections to County Government networks must pass through a network firewall. Each network firewall must have a rule set specific to its purpose and location on the network. Network firewall configuration rules and permissible services rules must not be changed unless there is a justifiable reason. Any change to an external connection or to the configuration of the firewall must be adequately tested and documented.

All County Government network firewalls must be physically located in ICT data centres and accessible only to those whose roles and responsibilities permit them to access network firewalls. These secure spaces must also have adequate physical security measures installed.

An audit of network firewalls will be done bi-annually. These audits must also include the regular execution of vulnerability scanning on server security

Services and applications on the server that will not be used must be disabled. Access to enabled services shall be logged and/or protected through access-control methods such as TCP wrappers.

Trust relationships between systems are a security risk, and should not be used for any servers. Always use standard security principles of least required access to perform a function. Root shall not be used when non-privileged account can suffice.

Servers shall be physically located in an access-controlled environment and privileged access shall be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

The Director ICT will facilitate the process of keeping the software up to date with the latest software releases from the vendors (if operationally feasible), so that patches that fix security bugs are installed in a timely manner. The most recent security patches must be installed on the server as soon as practical, the only exception being when immediate application would interfere with applications running on the server.

System Administrators should be very cautious about root password or Administrator password. The password should not be stored as plain text or written down on paper. Encryption utilities should be used if the password has to be stored in a file for some reason. A back up of the file should be stored on paper or other media in a physically secure place such as a safe which is accessible to someone of integrity, but who does not do routine system administration.

Remote Access

It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to County Government internal networks through their accounts.

VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

All computers connected to County Government internal networks via VPN or any other technology must use the most up-to-date anti-virus software and by using VPN technology with personal equipment, users must understand that their machines are a de facto extension of County Government network, and as such are subject to the same rules and regulations that apply to County Government owned equipment.

Mobile computing and storage devices containing or accessing the information resources at County Government must be approved prior to connecting to the County Government's information systems. This pertains to all devices connecting to the network regardless of ownership. Mobile computing and storage devices include, but are not limited to: laptop

computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device that may connect to or access the information systems at County Government.

Encryption Policy

Devices and Media Requiring Encryption: Encryption is required for all laptops, workstations, and portable drives that may be used to store or access sensitive data. The IT department will provide, install, configure, and support encryption where it is needed.

Electronic Data Transfers: Any transfer of sensitive data shall take place via an encrypted channel. If the encryption method includes a password, that password must be transferred through an alternative method, such as calling the individual. Email messages containing encrypted data may never include the password in the same message as the encrypted data.

Physical Transfer of Electronic Data: Any time sensitive is placed on a medium such as a CD, DVD, or portable drive to facilitate a physical transfer that data must be encrypted. Archiving sensitive data to a physical medium is not recommended, but is permitted if the data is encrypted. All archiving shall be done electronically, so that it is stored in a controlled data centre and backed up by the IT department.

Internet and E-mail

Access to the Internet is provided to County Government staff for the benefit of the county. Staff members are able to connect to a variety of information resources globally. Conversely, the Internet is also full of risks and inappropriate material. This policy will be used to ensure that all County Government staff members are responsible in the use of the internet.

Granting of Internet Access

Users who access the Internet shall ensure effective, ethical, and lawful manner access. Persons requiring special services, which consume considerable bandwidth such as streaming, must obtain an authorization from the Director ICT and his/her supervisor.

Acceptable use

Staff members using county Internet address are representing the county. They are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

Accessing databases for information as needed.

File downloading and uploading (File Transfer Protocol (FTP)).

Remote access (SSH, VPN, Terminal services, Citrix).

Communication tools (Email, IM, Voice and Video).

Collaboration tools (Groove, online presentations, discussion groups, blogs, wikis, Feeds).

Video and sound streaming.

Access to Intranet sites, systems and facilities.

Unacceptable Use

Staff members must not use the Internet for purposes that are illegal, unethical, harmful to the County Government, or non-productive.

Examples of unacceptable use are:

Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.

Conducting personal business using county resources.

Transmitting any content that is offensive, harassing, or fraudulent.

Misusing, disclosing without proper authorization, or altering personnel information (e.g., making unauthorized changes to personnel files, or sharing personnel data with unauthorized personnel).

Any unauthorized, deliberate action that damages or disrupts computing systems or networks; alters their normal performance, or causes them to malfunction.

Wilful or negligent introduction of computer viruses, worms or other destructive programs into Institution systems or networks or into external systems and networks.

Unauthorized decryption or attempt at decryption of any system or user passwords or any other user's encrypted files.

Packet sniffing, packet spoofing, or use of any other means to gain unauthorized access to information, a computer system, or network.

Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.

Unauthorized downloading of any shareware or freeware programs or files for use without authorization in advance from the user's supervisor or ICT office

Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violates any national or international laws, and regulations.

Deliberate pointing or hyper-linking of institution Web sites to other Internet / WWW sites whose content may be inconsistent with or in violation of the aims or policies of the county.

Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls and authorization.

Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

Any ordering (shopping) of items or services on the Internet.

Playing of games or initiating hoaxes.

Any form of gambling.

Forwarding of chain or hoax letters.

Accessing pornography sites.

Accessing hacker sites.

Participation in any on-line contest or promotion sites

Acceptance of promotional gifts.

Use of Internet facilities to issue statements or opinions on any subject on behalf of the county or on behalf of other individuals unless all parties have endorsed these statements.

Requesting, accessing, posting, or downloading of any material that incites crime or terrorism (as defined in either the receiving hosting country, or any country through which the information is routed).

Website Advertising

Third-party products or services shall not be advertised or promoted in the county's website without prior written approval from the Executive Committee Member. Other than that, links to external websites shall not be established without prior written approval from the management.

The content of the county's website shall only be changed or updated by authorised personnel and sensitive in-house information shall not be posted on the county's website.

The county reserves the right to access the contents of any messages sent over its facilities if the County Government believes, in its sole judgment, that it has a need to do so.

Audit Trails

The IT systems shall ensure that relevant information (an audit trail) about actions performed by users, or processes acting on their behalf can be linked back to the user and the user held accountable. The systems shall protect this audit trail from unauthorized access or modification.

The audit trail shall provide end-to-end user accountability for all security relevant events and must be traceable for the lifetime of the request or activity.

The systems shall, by default, cause a record to be written to the security audit trail for at least each of the following events (the IT Department may opt to not log some of these events due to operation constraints):

Invalid user authentication attempts.

Logons and activities of privileged users, e.g., ICT Director

Unsuccessful data or transaction access attempts.

Successful accesses of security-critical systems resources.

Changes to users' security profiles, privileges, or attributes.

Changes to access rights of resources.

Creating new accounts.

Changes to the systems security configuration.

Modification of systems software.

Modification of application software.

Modification of data (e.g. master files / transaction files).

For each recorded event, the audit record shall identify, at a minimum:

Date and time of the event.

User-id and associated point of physical access, e.g., terminal, port, network address, or communication device.

Type of event.

Name of resources accessed.

Success or failure of the event.

Old Value / New Value.

Actual or attempted passwords shall not be recorded in audit trails.

Audit control data, e.g., audit event tasks, must survive systems restarts.

To optimize on system storage, audit trails shall be archived to alternative storage locations at least monthly.

The Director ICT will actively ensure that security events are logged and monitor system activity and be aware of all aspects of the system, including what the normal load is, who has access to the system, days/times when different individuals access the system, etc.

Only the Administrators group shall have the right to manage auditing and security logs.

Network systems will be monitored to ensure conformity to access policy and standards. This is necessary to determine the effectiveness of measures adopted and to ensure conformity to an access policy model. The county reserves the right to monitor all traffic on the County Government network. Any or all users, PCs, terminals, network addresses, user ID's, email or other network traffic may be monitored at any time for compliance with security controls and policy.

High risk data must be encrypted during transmission over insecure channels. Confidential data shall be encrypted during transmission over insecure channels.

Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of or re-purposed, data must be certified deleted or Disks destroyed consistent with industry best practices for the security level of the data.

Wireless Policy

All wireless infrastructure devices that reside at any County Government office site and connect to County Government's network, or provide access to information classified as confidential or sensitive shall:

Be installed, supported, and maintained by an approved support team.

Use approved authentication protocols and infrastructure.

Use approved encryption protocols.

Maintain a hardware address (MAC address) that can be registered and tracked.

Not interfere with wireless access deployments maintained by other organizations.

IT Configuration and Patch Management

Overview

As county government becomes increasingly dependent on Information Communication Technology solutions to support critical processes, it also increases its exposure to security and other software vulnerabilities.

Principles

IT configuration and patch management process is part of County Government's overall IT security strategy. All service provider agreements must contain an adequate configuration management process. Oversight and accountability is the responsibility of county and any contracted Service Providers.

Requirements

The following are mandated for a configuration and patch management process:

Configuration Management

Provides assessment of asset compliance.

Identifies non-compliant assets.

Creates a plan to bring non-compliant assets into compliance.

Executes the plan.

Provides Assurance of Compliance: the Service Provider must provide documentation that assets are in compliance to the County Government IT security standards.

Patch Management

Vulnerability identification and remedies (e.g., patches, etc): The County Government or its designated service provider will proactively monitor for vulnerabilities and patches for all software identified in the system inventory.

Prioritization of Patches: The County or its service provider must prioritize the set of known patches and provide classification to sectors, regions, and units on the criticality of each patch.

Risk assessment: When the County or its designated service provider discovers vulnerability and a related patch and/or alternative workaround is released, then the County or its designated service provider will consider the importance of the affected assets and/or area of operations, the criticality of the vulnerability, and the risk of applying the patch.

Change Control: The County or its designated service provider will follow the standard Change Control procedure for application of any changes to configuration.

Assurance of Deployment: The Service Provider must provide documentation that patches have been effectively deployed to all applicable environments and/or infrastructure.

Incidence Handling and Response

All ICT systems or User support related Incidents shall be reported to ICT office and necessary action shall be taken as per the ICT incident handling procedure.

The ICT officer in charge shall ensure that all incidents are resolved in timely manner and respective user be notified

In case of any system down time or scheduled maintenance, the ICT office shall ensure that all members of staff and affected users are notified

Reportable incidents: Incidents which must be reported include IT systems errors and failures, email and internet errors, network and antivirus issues, violations of security policies and standards by other County

Government employees or contractors, and attempts to access County Government information resources by unauthorized personnel.

3 Risk Management

Overview

Risk analysis involves examining the probabilities and the possible consequences of undesirable events that would negatively impact County's Information. It identifies threats to be managed in the context of risk management. Risk management aims to reduce, but not necessarily eliminate, the frequency of a threat and its impact if it occurs. Risks can be accepted, transferred, or reduced.

General Principles

Risk Analysis

In general, risk analysis is comprised of four major activities:

Identification of potential negative impacts or those risks that could compromise County's activities

Threat assessment or the determination of the likelihood of the threat

Vulnerability assessment or the determination of the degree of seriousness of the weakness that could be exploited;

Risk assessment, which is the result of the combination of asset valuation with the levels of potential threats and vulnerabilities to form measures of risk. Threats can be accidental, such as software malfunction or natural disaster, or deliberate, such as disgruntled persons and computer hackers.

Risk Management

Risk management identifies the countermeasures to be implemented in order to reduce risk to an acceptable level. One of the purposes of these practices is to identify a common set of countermeasures to protect County Government Information.

In order to effectively protect the information, environment and data belonging to County Government; the concept of "need-to-know" must be implemented. Need-to-know supports authorized access and sharing of County Government Information within and across business functions for those who can demonstrate a legitimate business need and obtain access

approval from the County Government unit responsible for the County Government Information.

Requirements

Risk analysis should involve some quantitative or qualitative methodology to determine threats, vulnerabilities, impacts, and measures of risk.

Risk management for County Government Information requires a set of common, cost-effective controls including:

Utilization of individual access security controls within applications, systems, and infrastructure of County Government's computing and communication resources;

Limits on access to all County Government Information based on need-to-know;

Assurance through audit trails of system and application access, edit, and delete activity; and

Provisions for on-going employee and user awareness.

Monitoring and Evaluation

Internal Audit (IA) will be charged with the responsibility of reviewing the risk management practices within the ICT function.

The IA function shall:

Review the process of risk identification within ICT and assess the adequacy of the process and risk register developed from the process; and

Review the adequacy of controls designed to mitigate against the risk and test the operating effectiveness of those controls over a defined period of time.

4 Privacy and Data Protection Policies

All County Government Information is "proprietary", that is, the property of County Government or applicable third parties that County Government has an interest in protecting wherever it exists, regardless of location or storage medium e.g. personally owned computing equipment, third party owned computing equipment, IPAD, tablets or Cell Phones. This information must be protected by County Government employees, and users, and service providers against unauthorized disclosure, modification, compromise, or destruction.

Protections for County Government Information are supported by implementing the concept of need-to-know. Need-to-know supports authorized access and sharing of County Government Information within and across functions for those who can demonstrate a legitimate need and obtain access approval from the Information Owner responsible for the County Government Information.

Some County Government Information is sensitive and/or could create adverse consequences if disclosed and therefore needs additional protections beyond those mandated for all County Government Information.

All information resources shall be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection shall be consistent when the data is replicated and as it flows through the County Government. Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to this classification. Three classes of classification are:

Critical/High Risk: Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Payroll, personnel, and financial information are in this class. Other data may need to be treated as high risk because it would cause severe damage to the County Government if disclosed or modified.

Confidential/Medium Risk: Data that would not expose the County Government to loss if disclosed, but that the data owner feels shall be protected to prevent unauthorized disclosure.

Public/Low Risk: Information that may be freely disseminated.

Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.

5 Physical and Environmental Controls

All IT infrastructure and technology shall be protected by access control techniques that are appropriate for their criticality or sensitivity. Access to any County Government computer facility, IT infrastructure or technology component shall be restricted to authorized personnel only. Specifically, data centres / Server room shall be secured and access limited only to authorize personnel at all times and visitors' logs shall be maintained.

Physical security controls shall be in compliance with all local, regional, fire and safety regulations, as well as insurance requirements.

Measures shall be taken to minimize the risk of a fire from occurring within an installation, or from spreading into the installation from an adjoining area.

All Data Centres require clean, temperature/humidity-controlled air, which must meet computer manufacturer's specified temperature and humidity ranges.

All computer installations must have a dependable, consistent electrical power supply that is free from surges and interference, for all computer, air conditioning and security systems. A backup power supply shall be considered for the computer systems such as an uninterruptible power supply (UPS System).

Users must employ all reasonable means to physically secure their laptops when not in use, including using locking devices where provided. Users need to secure their laptops in the workplace, at a residence, while travelling or when left in a vehicle. Users must not access classified County Government Information in a public place, e.g. on a train, aircraft or bus if it can be viewed by others.

6 Change Management Policies

Software Change Control covers the control of all aspects of County Government IT systems software including the operating system its associated packages (DBMS etc.) and utilities, third party and locally developed applications, together with any command procedures and documentation to support and run them.

Change Management aims to manage the process of change and consequently limit the introduction of errors and so incidents related to changes. The objective of Change Management is to ensure that standard methods and procedures are used, such that changes can be dealt with quickly, with the lowest possible impact on service quality. All changes should be traceable, in other words, one can answer the question, 'what changed'?

After recording the Request for Change (RFC), IT staffs responsible for the making the change will make an initial assessment to check if any of the RFC's are unclear, illogical, impractical or unnecessary. Such requests are rejected, stating the reasons. The person who submitted the request should always be given an opportunity to defend his or her request.

All change requests shall be done as per the Change request procedure.

Obligations

When changes are required to systems software, associated packages and utilities, applications software, command procedures, or documentation, it is essential that the changes are:

i. Appropriately authorized and approved

ii. Thoroughly tested

iii. Sufficiently documented and

iv. Implemented at an appropriate time.

v. Any change must only be transferred into the production environment when approved by the appropriate System Custodian.

vi. Sound software security management requires the procedures to manage the change control for applications and systems changes are clearly defined. There must be a set of Software Change Control Procedures to assist the process.

vii. All operational software relating to strategic systems should be placed under appropriate Configuration Management.

Change Control Responsibilities

Specific personnel will be given the responsibility for the implementation of changes by undertaking appropriate testing in the test environment, and, subject to the appropriate approvals, moving the changes to the production environment. All elements of the system will be subject to Software Change Control Procedures.

There should be a separation of responsibilities in the transfer of software from test into the production environment. Any change request will be analyzed by an officer then tested by a different officer before implementation.

Change Control Environment

Two separate environments should be maintained for all County Government systems:

Testing

Production

Migration of software between environments should only be undertaken after obtaining the appropriate sign-offs as specified in the Software Change Control Procedures.

New or modified software should be transferred to the Testing Environment for systems and acceptance testing by an appropriate testing group, according to an agreed test procedure.

Following successful completion of testing and approval by the appropriate systems custodian, the new or modified software should be transferred to

the Production Environment for implementation under the control of its Operations staff. A contingency plan to enable the software to be restored to its previous version in the event that the implementation is unsuccessful should be prepared where appropriate.

Documentation

The following documentation must be maintained;

Software Change Request: - No software change is to be undertaken without appropriately authorized Change Request as per change request procedure.

Technical, Operations and End User Documentation: - Appropriate documentation in respect of each software change must be completed in sufficient detail and accepted before the change is implemented in the production environment.

The following guiding principles should be applied in change management

Impact Assessment, Prioritization and Authorization - Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorized, prioritized and authorized.

Emergency Changes - Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process.

Change Status Tracking and Reporting - Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in process changes, and complete changes. Make certain that approved changes are implemented as planned.

Change Closure and Documentation - Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.

Training - Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training

and implementation plan and associated materials, as part of every information systems development, implementation or modification project.

Test Plan - Establish a test plan based on organization wide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.

Implementation Plan - Establish an implementation and fallback / back out plan. Obtain approval from relevant parties.

Test Environment - Define and establish a secure test environment representative of the planned operations environment relative to security, internal controls, operational practices, data quality and privacy requirements, and workloads.

System and Data Conversion - Plan data conversion and infrastructure migration as part of the County's development methods, including audit trails, rollbacks and fall backs.

Testing of Changes - Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.

Final Acceptance Test - Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan.

Post-implementation Review - Establish procedures in line with organizational change management standards to require a post-implementation review as set out in the implementation plan.

7 Asset Management

Copyrights and License Agreements

Policy Statement

It is County Government's policy to utilize firm approved and supported software and hardware, upgrade and maintain software and hardware, manage and maintain an inventory of owned assets and comply with all laws regarding software licensing and intellectual property. This directive applies to all software that is owned by County Government, licensed to County Government, or developed using County Government resources.

IT Department will:

Maintain inventory records.

Periodically scan County Government computers to verify that only authorized software is installed.

Ensure that all licenses are valid and renewed upon expiry.

Safeguard hardware and data.

Account for IT assets and configuration items.

Verify configuration records and correct exceptions.

Maintain logical and physical security.

Ensure there is no use of unauthorized and illegal duplication of software.

For all assets, owners should be identified and the responsibility for the maintenance of appropriate controls should be assigned.

All Assets will be insured

In case of any Asset Loss, the officer in-charge should report immediately, ensure all documentation and procedures are followed to enable re-placement

Data owners will:

Classify assets.

Implement specific controls for protection of assets.

Shared ICT Resources

All shared / pooled ICT resources including Laptops, Cameras, Projectors and printers shall be centrally managed under ICT office and accessible to all authorised County Government staff. Records of issues shall be maintained. In event any of these resources needs to be used out of office, a dully authorised gate-pass form shall be filled.

Acquisition Guidelines

Procurement Control

County Government utilises centralised procurement system under procurement department. ICT department's function is to provide specifications to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business

Software Acquisition Guidelines

The Information Technology department must be notified of all new software by user departments. The IT Department reserves the right to refuse software if it presents any risk to the County.

There are 3 types of software available to County Government employees:

Pre-approved Purchase Software: Software commercially marketed, developed by an organization outside of County Government. County Government IT Department maintains a current list of these titles.

Specialized Purchase Software: Software developed by a vendor to perform a unique function that cannot be accomplished using pre-approved purchase software. This software requires a capital appropriation and the ICT director's approval.

In-house Developed Software: An application or system designed specifically by and for County Government. Prior to development of a system, the System Administrator must be contacted to determine if

similar systems can be utilized to fulfil requirements and no duplication of effort is involved. All County Government development standards must be followed.

Prior to the selection of the second or third option, the System Administrator must participate in a build versus purchase analysis that is based on the total inventory and resource of systems within County Government.

All security software shall be selected by the Information Technology and Internal Audit departments. Any new operating system or operating environment (e.g. Windows 8) must be approved by IT Department prior to acquisition.

Hardware Acquisition Guidelines

Acquisition of ICT hardware equipment's is centralized. This provides a clear approach to ensuring efficient hardware purchases

All signed requests associated with a specific purchase for personal computer equipment must be forwarded through ICT office for compiling, specification development and onward transmission to procurement section as per procurement procedures.

During PC maintenance, the user shall be cautioned that under certain repair situations sensitive data would be vulnerable. This condition occurs when there is a failure of a hard disk necessitating its removal and replacement. If a hard disk must be removed because of problems, the user or a technician shall attempt to perform a low level format, which will erase all the information. If a low level format cannot be performed successfully, then the damage to the disk is usually extensive and consideration shall be given to physically destroying the media. Encryption will also provide protection to ensure that data is not retrievable during a repair situation.

Disposal Guidelines

County Government Information stored on any form of electronic media must be electronically destroyed by magnetically erasing (e.g., degaussing)

or reformatting the media by rewriting over the media. Normal "delete" commands simply delete the address reference to the start of the file but leave the data intact. County Government must have assurance that when electronic data is deleted and/or disposed of, that the process includes complete destruction of the data so it cannot be read or reconstructed to be read in any readable format. County Government data must be protected against unauthorized disclosure during the disposal process.

Any failed disk drive that requires data recovery, appropriate authorization must be obtained prior to the disk being sent out to an external data recovery company.

When replacing a defective storage, it is required that electronic degaussing take place before the defective hard drive can be sent out for repair or scrapped. A log must be created and kept of all hard drives sent off-site for repair or scrap indicating the date when degaussing took place and by whom.

Assets register:

An assets register will be maintained for all County Government software, software licenses and Computer hardware. This register will be updated when any of this assets is acquired or disposed and will be reviewed twice a year to ensure that it remains accurate.

8 Business Continuity Management Policies

Overview

Disaster recovery is a proactive planning process to manage the potential loss of County Government Information or inability to access County Government Information in the event of a disaster. Disasters may be immediate, significant, and obvious, or they may be more insidious and negatively impact County Government over a period of time. As County Government becomes more dependent on its computer and communications resources, the loss of these resources could cripple the County in a few hours. The focus of Business continuity management shall include the following;

Backup Policy

Software: All server software, whether purchased or created personally should be backed up at least once a month.

System data: System data is to be backed up at least once a week.

Application data: All application data should be backed up using daily incremental backups and weekly full backups.

Storage: All backup media must be stored in a safe and secure location extraneous to the location of the backed up systems. All backup media must be stored in a fireproof safe. All software full backup and monthly backup media must be stored in an off-site backup archive storage location.

Data Retention

County Government will establish a hierarchy of backup cycles. A full daily backup cycle involving retaining a sets of backups will be maintained. One of daily backup is retained as part of backup cycle and stored in a local safe.

End of fiscal year and yearly archive data backup shall be generated in multiple copies and each copy stored in a distinct archive storage location

and stored in perpetuity. In this way, the risk of catastrophic loss is minimized at a reasonable media cost.

Electronic records will be retained for 7 years before they are disposed.

Media Storage

For safety, backup media shall be stored in a fireproof and protected location. In the case of magnetic media they shall be in a case or vault that is shielded from electro-magnetic radiation. For maximum safety the archive media shall be stored at a site that is remote from where the tapes are used

Restoration of Data

The restoration of data using data backups must be tested at irregular intervals (a minimum of once a quarter is recommended) and at least after every modification to the data backup procedure. It must at least once be proven that complete data restoration is possible. This ensures reliable testing as to whether:

i. Data restoration is possible.

ii. The data backup procedure is practicable.

iii. There is sufficient documentation of the data backup, thus allowing a substitute to carry out the data restoration if necessary.

iv. The time required for the data restoration meets the availability requirements.

Disaster Recovery

Disaster Recovery Planning (DRP) is the preparation and testing of plans to recover from a disaster. DRP supports County Government's overall plan to ensure the continuity of the total operations in the event of a disaster. The detailed contents of the DRP will depend on the nature and criticality of the systems (those applications / systems that support critical operations) described the value and sensitivity of the County Government Information involved, and the potential impacts resulting from identified threats. The

DRP must provide a complete, consistent, and practical statement of all actions, roles, and responsibilities, prior to, during, and after a disaster to:

Ensure minimum disruption to the performance of the affected business unit while allowing County Government to function;

Reinstate County Government computing and communication resources based on the stated priority order within time limits specified by County management.

9 Incident Management

Incident Management is a reactive task, i.e. reducing or eliminating the effects of actual or potential disturbances in IT services, thus ensuring that users can get back to work as soon as possible. For this reason, incidents are recorded, classified and allocated to appropriate specialists; incident progress is monitored; and incidents are resolved and subsequently closed.

In this context, 'Incidents' include not only hardware and software errors, but also Service Requests - because both are handled in a similar way. That is, Incident Management handles their complete life cycles.

Service Requests can be made for 'standard services': that are agreed to be provided under SLA's are delivered through agreed procedures which have appropriate checks and controls; and where records are maintained.

The following guidelines apply for incident management;

Employee Reporting Requirements: All employees of County Government are responsible for maintaining a familiarity with the information security policies, standards and guidelines and are responsible for reporting any suspected security breaches or violations and system failures.

Recipients of Reports: Employees who suspect a security breach or violation will communicate their concerns to their direct supervisor or other official in their supervisory chain. This individual must then evaluate the allegations and refer severe violations to the information management executive.

Timeliness of Reporting: Systems failures and Security breaches will be reported in a timely manner based on the severity of the incident and the nature of the data involved.

Provision of Violation Information to Owners: The information security manager is responsible for summarizing and reporting data security violations to data owners on a timely basis.

Reportable incidents: Incidents which must be reported include violations of security policies and standards by other County Government

employees or contractors, and attempts to access County Government information resources by unauthorized personnel.

Subsequent to resolution of major incidents, IT should carry out a root cause analysis to identify what caused the incidence and ensure that the cause has also been addressed

Network Security Monitoring

Purpose of Monitoring: Systems will be monitored to ensure conformity to access policy and standards. This is necessary to determine the effectiveness of measures adopted and to ensure conformity to an access policy model.

County to Monitor: County Government reserves the right to monitor all traffic on the County Government network. Any or all users, PCs, terminals, network addresses, user ID's, email or other network traffic may be monitored at any time for compliance with security controls and policy.

Publication of Monitoring Policy: To maximize the effectiveness of auditing, unit managers will publicize the fact that it is County Government policy to audit network activity.

Authorization of Monitoring Activities: Company management must formally authorize all monitoring activities.

Control of Network Monitoring Devices: Only authorized personnel can use network diagnostic test hardware and software such as sniffers and monitoring devices to monitor traffic on the County Government network. Information owners should be notified when non-routine network monitoring devices are used to monitor their data.

Monitoring of System Use: Unit managers will implement procedures for monitoring system use. Such procedures are necessary to ensure that users are only performing processes that have been explicitly authorized. The level of monitoring required for individual systems will be determined by a separate risk assessment. Areas that will be considered are:

i. Access failures.

ii. Review of logon patterns for indications of abnormal use or revived user IDs.

iii. Allocation and use of accounts with a privileged access capability.

iv. Tracking of selected transactions.

v. The use of sensitive resources.

vi. Dial-up activity.

vii. Firewall activity.

viii. OS and application access attempts.

ix. Security administration activity

Use of Intrusion Detection Systems

Requirement for Use of Intrusion Detection Systems

The use of intrusion detection systems to perform real-time analysis of network traffic patterns to detect attempted attacks is required for Internet connections and encouraged within the internal network. Without intrusion detection software or hardware it is more difficult to detect attempts to breach security, as well as certain types of sophisticated attacks, thus increasing the likelihood of undetected compromise of system integrity and confidentiality.

Real-time Intrusion Detection on Public Access Systems: Firewalls must utilize system monitoring tools that provide real-time alerts whenever suspicious user activity is detected.

Response to Intrusions/Attempts: Unauthorized attempts (either successful or unsuccessful) to access or modify data protected behind the firewall will be promptly investigated by system administration and information security personnel.

Compliance Monitoring

IS Compliance Review Program: The Director of ICT in liaison with Internal Audit function is responsible for establishing a program to continually monitor the County Government system security environment

for compliance with published information security policies, standards, and procedures. This will include an assessment of user practices, operations, and systems configurations.

Environmental Compliance Program: The County Government is committed to respect and adhere to all environmental laws in existence. More importantly to ensure that all ICT infrastructures being put in place are done by use of environmentally friendly materials. It is in turn expected that the County Citizen will allow the County Government any necessary wayleaves to pass through the private land. The County Government will in turn provide service accessibility to these Citizens at subsidized rates. The Government will also ensure that e-waste arising from ICT is disposed off as recommended in the environmental laws in place.

10 Human Resources Function

The HR section is responsible to maintain IT personnel recruitment processes in line with the overall organization's personnel policies and procedures (e.g., hiring, positive work environment, orienting). Implement processes to ensure that the County has an appropriately deployed IT workforce with the skills necessary to achieve organizational goals.

Evaluate staffing requirements on a regular basis or upon major changes to the business, operational or IT environments to ensure that the IT function has sufficient resources to adequately and appropriately support the business goals and objectives.

Personnel Competencies Staffing of Roles - Define, monitor and supervise roles, responsibilities and compensation frameworks for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned.

Personnel Training - Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational goals.

Dependence Upon Individuals - Minimize the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.

Personnel Clearance Procedures - Include background checks in the IT recruitment process. The extent and frequency of periodic reviews of these checks should depend on the sensitivity and/or criticality of the function and should be applied for employees, contractors and vendors.

Employee Job Performance Appraisal - Require a timely evaluation to be performed on a regular basis against individual objectives derived from the County's goals, established standards and specific job responsibilities.

Employees should receive coaching on performance and conduct whenever appropriate.

Job Change and Termination - Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimized and continuity of the function is guaranteed.

Contracted Personnel - Ensure that consultants and contract personnel who support the IT function know and comply with the County's policies for the protection of the County's information assets such that they meet agreed-upon contractual requirements.

11 Monitoring and Evaluation

The Information Communication Technology Policy is the responsibility of the ICT Director. These policies will be reviewed and evaluated annually for updates. Updates may include the creation of new policies, modifications to existing policies, and/or the deletion of line item details. Updates can be triggered by several events including but not limited to new technology, security deficiencies, changes in legal, regulatory, or reporting requirements, physical or environmental alterations, changes in business demand, request for deviation from a service provider and periodic re-evaluation of current requirements

12 Conclusion

This policy aims to define a governance and management structure for the development and implementation of ICT policies, strategies and services; and define the role of the County's Information and Communication Technology Unit.

It provides governance framework for the County's ICT services in relation to best standards.

The County should develop an ICT strategy with a detailed implementation matrix to facilitate full execution of the ICT policy.