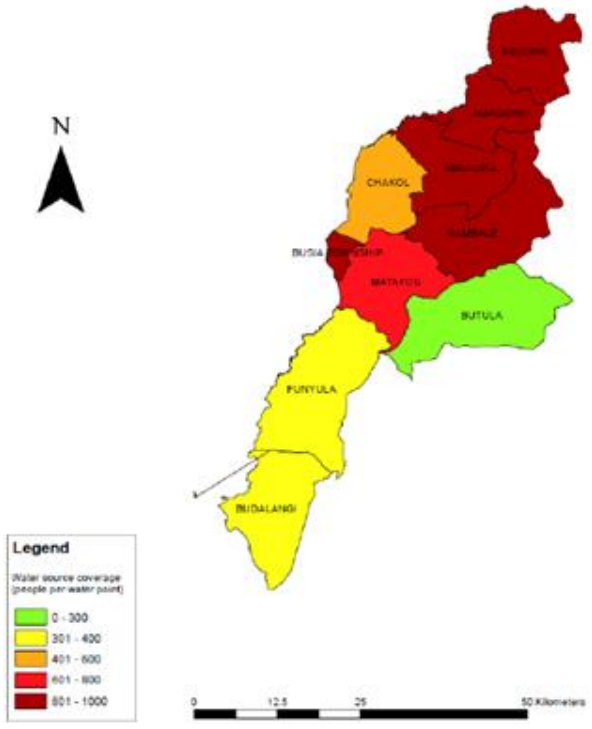
Draft 3: Busia ICT Systems and Services Standard Operating Procedures (SOP)

November, 2015



PART 1 – SIGN-OFF AND APPROVALS

Project: Busia ICT Systems and Services Standard Operating Procedures (SOP)

Sign-off for: Busia ICT Systems and Services SOP - Draft Three

County: BUSIA

	_____	**Accepted**
Sign-Off:	_____	Accepted with Modifications
	_____	Not Accepted
Signature:	_____	
Name (Capitals):	_____	Date _____
Position:	…… of ICT	In charge
Signature:	_____	
Name (Capitals):	_____	Date _____
Position:	Governor	
Signature:	_____	
		Date _____

Busia ICT Systems and Services SOP

- Access Control
- Anti-malware & Anti- Spyware
- Email and Messaging
- Internet Use
- Social Media
- Network Management
- Password
- Security
- Software Licensing Management
- Data Management
- Remote Access & Mobile Computing

Date First Created:
October, 2015

Last Approval Date:
November, 2015

Next Review Due: March 2018

Requires Approval (yes/no): Yes

Previous Reference (for control purposes):

2015 ICT Systems and Services SOP

1.0 Background

1.1 The County regards Information systems and the information they contain, of vital importance to its efficient functioning. The systems and the associated information processing tools and services – including desktop productivity tools, e-mail, web-based systems and the underlying network – now pervade all functions of the County.

1.2 Security of information is an essential requirement in any government entity. The procedures contained in this ICT Services SOP aim to ensure security of information.

1.3 The procedures should be followed in conjunction with the Government of Kenya laws and procedures.

2.0 Scope

2.1 These procedures apply to all **authorised users** of County information systems (staff and other stakeholder users).

3.0 Summary of ICT Systems and Services Procedures

The following are set out below:

The Communication Plan and review information for this SOP can be found here

4.0 Access Control Procedure

4.1 Requirement for access controls

The county government requirements for access controls on computer systems are:

- Protection of sensitive, personal or confidential information from unauthorised access.
- Ensuring data integrity in terms of preventing deliberate or accidental modification or deletion.

4.2 Access Control Rules

All Users

- The county government requires that authorised access to any computerised information system by staff and other stakeholders parties must be controlled by an appropriate level of access.
- The rules for access to computerised systems are as follows:
- Users can only be granted authorisation to shared information after approval has been given by an authorisation authority (i.e. ICT head).
- Access will be controlled via pre-determined access levels. Authorised users will be assigned the approved level of access by the system administrator for the system that access is sought.
- Access granted must only be to very specific information and must not include any access to information that the user does not require access to.
- The type of access, (i.e. read, write etc.) in cases of access to shared information, must be established prior to granting access.
- Access is dependent upon each user having a unique computer user account and password. Creation of accounts for staff are dependent upon authorisation from Human Resources which includes completion of the county government's Acceptable Use Policy.
- Stakeholder account creation is dependent upon departmental acceptance of the terms of the county government's Acceptable Use Policy.
- User accounts of users who have changed job function, or who have left the county government will be disabled upon notification from the Human Resources Department

Access Control Rules – System and Network Administrators

System and network administrators will be permitted the highest access levels to information within their information system or domain provided that:

- Such access is required to administer and manage the information system, information store or network domain.
- Strict observance of data confidentiality is practised.
- Strong passwords are selected as per guidelines issued in the county government Password SOP.

4.3 Types of Access Control Employed

The type of access control that will be used include:

Information System Controls

Each user must be given approval to have access to a system by the System Administrator. The appropriate access level will be determined by the System Administrator and agreed with the user's chief officer before the access level can be assigned.

File System Controls

Access to centralised file systems such as folders of documents on file or storage servers will be permitted via profiling and network security group access.

Computer System Controls

Use of security controls such as Microsoft's Group Policy will be used to control access to Personal Computer operating system files, admin tools and to prevent installation of software.

Network Controls

Protection of the county government network will be achieved by the use of firewalls, access control lists and where appropriate VLANS (Virtual Local Area Networks).

4.4 Monitoring and Review of Access

System and Network managers will review at least annually the access levels pre- configured for each system and also the access level that has been granted to each user for the information system, information store or network domain.

4.5 Reporting of Incidents

All users have a responsibility to report to appropriate system managers:

- Access still granted but no longer required to a system.
- Excessive or inappropriate access to a system.
- Misuse of access to a system by another user.

5.0 Malware – (viruses, ransomware, worms, trojan horses, spyware)

5.1 Introduction

The increased growth and dependence on ICT systems necessitates in appropriate support, security and contingency arrangements being in place to ensure system reliability and availability. One of the greatest risks to system stability and data integrity has been the growth in number and prevalence of malware software

Definitions of Main Malware Types

- Virus - is a computer program designed to cause corruption or destruction of other computer applications and data. It usually infects an existing program
- Ransomware – is a program that encrypts data on the victim's computer. The perpetrator behind the attack issues instructions on how to recover the data. Usually payment is demanded in the form of a virtual currency such as bitcoins.
- Worm – is a computer program that replicates itself on the host computer and often will attempt to spread to computers on other networks.
- Trojan horse – is a computer program which disguises itself to appear useful or interesting in order to persuade a victim to install it. They can be used by criminal elements to create a "backdoor" to a computer for purposes of stealing personal or financial information, or to provide a means to have control of the infected computer.
- Spyware – is a computer program that records or captures information from an infected computer without the knowledge of the computer user

With the onset of web and e-mail services, malware can spread across multiple organisations and countries very quickly. The most common method of infection today is via infected file attachments on e-mail messages.

5.2 Susceptibility

Organisations most susceptible to infection, are those who either do not have any anti-malware or anti-spyware software, or who do not take adequate measures to ensure that the software is kept updated on servers and other ICT devices. Furthermore, organisations who interchange information regularly between employees or indeed other organisations increase the likelihood of infection spreading.

5.3 Preventative Measures

The county government uses a commercial anti-malware product that provides coverage for all servers, PCs and laptops. The product is updated on all servers and desktops directly when latest updates are available from the vendor's web site. Non-protected devices are proactively identified by the software permitting viral infection weaknesses to be exposed and dealt with. However, it is not acceptable to rely on the anti-malware product alone to prevent a viral outbreak. There are a number of mandatory stipulations to be observed by staff and other stakeholders to ensure the risk of virus and spyware infections are kept to a minimum:-

- All Servers, PCs and laptops and other ICT devices brought on to any county government Centre must be properly configured for automatic updates and have up to date anti-malware software installed.
- It is not permissible to attempt the interrupting or disabling of automatic updates to the anti-malware software.
- All county government –owned laptops and PCs must be connected to the county government network at least once per week to facilitate anti-malware updates.
- Personally owned laptops and PCs must be kept updated with anti-malware software particularly if such devices are used to interchange information with county government systems.
- It is not permissible to copy/upload any material to any device on the county government network unless that device (i.e. PC or laptop) has the most recent anti-malware updates installed. Advice should be sought from the ICT Support unit if staff or stakeholder have any doubts as regards the integrity of data stored on portable media regardless of the media having been previously scanned.
- Only software procured and installed by the county government may be used on any county government owned ICT device. Installation and execution of any other type of software, including screensavers and games is prohibited.
- Use of peer to peer file sharing programs is strictly forbidden i.e., Kazaa, Limewire, Bear Share, due to the extremely high risk of virus introduction.
- Installation or use of spyware software is forbidden.
- It is not permissible to download any software from any spyware websites.
- Unexpected or suspect e-mail messages with or without attachments must be deleted immediately. Care must also be taken to immediately empty the Deleted Items folder.
- All users should monitor 'IT announcements' email for new virus or spyware alerts and take appropriate action.
- Downloading of any file type from unsolicited web sites is prohibited.
- It is the responsibility of all users of county government computing facilities to ensure that data stored on portable devices (i.e. laptops, Macbooks, tablets) or portable media such as USB drives or Smart Phones is backed up.

- Suspected virus infections must be reported immediately to the ICT Support unit.

5.4 Levels of Protection

Having anti-malware protection on servers and desktops provides multi-level protection in that material sent via e-mail or the web is scanned on the e-mail/web server before being accessed by client PCs. Furthermore, material loaded via portable media is scanned by the client PC and then scanned again by the anti-malware guarded file server.
All county government servers including domain controllers, file servers, firewall and any other on premise services must be protected with anti-malware software.

Additional protective measures include:

- Certain file types known to "hide" or contain viruses are blocked if included in e-mail attachments. Some examples include: .exe, .vbs, .com, .mdb.
- Macro security levels In MS Office suite are set to Medium or High.
- Prevention of software installation on ICT devices by using Microsoft Windows group policies.
- Infected file attachments on external e-mail messages coming into the county government are removed.
- Off-line content is deleted from PC/laptops after a successful login has taken place.

5.5 Reporting

Any indications of, or suspicions of virus or spyware activity must be reported to the county government ICT Support Unit.

5.6 Dealing with a Malware outbreak

Should a viral outbreak take place the following procedure will be followed:

- Head of ICT to inform Chief Officers of scope and scale of infection.
- ICT staff will attempt to isolate infected device(s).
- If required, infected devices will be disconnected from the network.
- If required, unaffected network segments will be isolated from infected segments.
- Virus- free device with latest anti-malware software will be used as a cleaning medium for cleansing of infected files. If feasible, a secondary anti-malware product will be used to ensure that infected material and devices have been entirely cleansed.
- Upon removal of the infection, all servers and networked PCs, laptops will be updated with the latest anti-malware updates.
- The "all clear" to be issued by the Head of ICT to Chief Officers.
- An investigation to be initiated by the Head of ICT as to the cause of infection. On completion, a report is to be produced and forwarded to the Chief Officer in charge of ICT, outlining appropriate countermeasures and safeguards.

5.7 Deliberate Malware Introduction

Whilst malware by nature is created to deliberately disrupt ICT services, often they are accidentally introduced to an organisation's ICT systems. The county government will initiate disciplinary action against any employee or stakeholder who either deliberately introduces, or attempts to introduce malware, or who is complicit with other parties or individuals in introducing or attempting to introduce a virus or spyware software.

5.8 Liability

The county government will not be deemed responsible for suspected loss of information in the course of ensuring that a malware free environment is maintained. It will also not be deemed liable if anti-malware software plus latest updates have been installed and have failed to prevent a viral infection occurring which results in loss or corruption of data, or loss of any ICT service.

5.9 Additional Security Recommendations (Personal PCs/laptops)

Keep Windows Firewall turned on at all times. This will stop unwanted access to the computer on the Internet (especially at home).

Ensure that some form of antivirus and anti-spyware software is running and that it is updated at least on a daily basis.

6.0 Email and Messaging Procedure

6.1 Introduction

All email and messaging users (staff and stakeholders) are bound by the terms and conditions of the county government's Computer Services Acceptable Use Policy. Note that "Messaging" includes any form of electronic messaging including instant messaging, text messaging and any form of web messaging service.

6.2 Acceptable use of Email and Messaging

The following guidelines must be adhered to:

- Users may access only their own mailbox and must not use, or attempt to access another mailbox. It is not permissible to send e-mail from another county government staff or stakeholders mailbox unless approval has been granted by both the mailbox owner and the sender's line manager.
- Users are discouraged from sending large file attachments to individual or multiple mailboxes to either internal or external recipients. "Large" can be defined as anything over 30MB.
- In order to reduce the risk of malware infection, users should not open file attachments of any file type unless:
    a. It is a Microsoft Office file (i.e. Word document, Excel spreadsheet) and
    b. It is a file that they are expecting to receive, or has been sent to them from a known and reputable source. *Please delete dubious mail messages or check with ICT Support unit for advice*

- Users must not e-mail or message any illegal, malicious or copyright protected files or information.
- Users are not permitted to use the county government email and messaging services as a medium to transmit offensive or abusive material or messages.
- Email should be used for county government of Busia business-related activities provided such activities are legal.
- Email spamming is forbidden. (Spamming is the forwarding on, or sending of unwanted e-mail to other users or groups of users without their prior knowledge or consent). The mailing of multiple users, or multiple mailing groups, or the mailing of one user or mailing group many times is also considered as spamming.
- Phishing e-mails must not be created or forwarded to others. Furthermore, phishing e- mails received that request personal (including passwords or usernames), financial or other confidential or sensitive information should be deleted.
- Each user is responsible for managing the content of their mailbox. There is an expectation that each user will delete processed messages from Mailbox folders. County government of Busia cannot guarantee the integrity and indefinite storage of mailbox information.
- E-mail can be set up and accessed on mobile devices such as mobile phones and tablet computers as long as the devices are secured in accordance with the terms of the Remote Access and Mobile Computing Standard Operating Procedure (SOP).
- All messages should be constructed observing acceptable etiquette. (For example, capital letters and large fonts should be avoided.)

6.3 **Dealing with Dubious or Suspicious Emails**

The most common forms of harmful or nuisance e-mail types are as follows:

- Messages that contain malware. There are e-mail messages which contain attachments that contain malware. The recipient is encouraged or instructed to open the attachment. Once opened, the malware is activated and will infect the recipient's machine and will in many cases attempt to spread to other machine by various means. Some malware can create their own e-mail address or can harvest other e-mail addresses and then send out to other recipients. As the sending e-mail address may well be the e-mail address of someone known to the recipient, they can be duped into opening the attachment.
- Messages that attempt to obtain personal or confidential information, (phishing). There are messages that try to convince recipients of the necessity to provide personal details such as banking details, user names and passwords. This can lead to loss of information, or to loss of money from bank accounts.
- Messages that contain hoax messages. There are messages that try to scare recipients into believing that a harmful virus is circulating and advise the recipient to pass the message on to other friends and colleagues. Messages encouraging recipients to pass on to many other recipients is often referred to as "chain mail". (The authenticity of hoax mail can be checked with leading anti-malware software companies via their web sites).
- Messages that flood many mailboxes (spam). There are messages that are generated with the sole intention of flooding mail servers so as to deny access to mail users. Such messages are referred to as spam.

There are many other forms of messages that circulate containing advertisements and other information which many would regard as "junk" mail. Some would also classify such mail under the category of "spam".

6.4 Breach of guidelines

Please note that breaches of above guidelines could result in the perpetrator(s) having their e-mail account(s) disabled. Serious offences could result in further disciplinary action being taken. County government Busia have the right to check material stored on computing facilities if it is suspected that acceptable use has been violated.

6.5 Staff and Stakeholder Leavers

Stakeholders will have their mailboxes deleted twelve hours after leaving the county government.

County government staff that leave the County will have their e-mail accounts disabled for three months and then their mailbox will be deleted.

7.0 Internet Use Procedure

7.1 Introduction

All Internet users (staff and stakeholders) are bound by the terms and conditions of the county government's ICT Policy. The county government uses web filtering software to block out prohibited sites and material. Should anyone inadvertently access any offensive or sexually explicit material, they should leave that site immediately and inform both their Chief Officer and the ICT Support Unit giving details of the URL visited.

As stated in the county government Busia ICT, county government of Busia have the right to monitor the transmission or storage of material through its computing services if it is suspected that acceptable use has been violated.

7.2 Acceptable Internet Usage

The Internet should be mainly used for county business related activities.

7.3 Unacceptable Internet Usage

The Internet should not be used for:

- Excessive personal use. (Personal use is permissible during break times).
- On-line gambling.
- On-line share trading.
- Accessing or downloading pornography.
- The obtaining and spreading of malware.
- Downloading or distributing copyright information.
- Downloading of software including games and screensavers.
- Posting confidential county government information or information about other employees or stakeholders.
- Abusing, harassing or criticising any other staff member, stakeholder or third party.
- Circulation of defamatory statements either from within or from outside of the county government.
- Deliberate overloading, or attempt at disablement of any ICT service.
- Downloading of large (over 3GB per file) video and audio files unless prior authorisation has been sought.

- The circumvention of county government ICT security measures.
- Accessing of chat rooms and social networking sites unless permission has previously been granted by Head of ICT.
- As a medium for transmission or receipt of abusive or offensive mobile phone text messages.
- Any other activity considered to be illegal or in breach of any county government policy or procedure.

Use of internet mail services such as Hotmail, Yahoo etc. should be avoided if possible. (Stakeholders and staff should use their county government e-mail accounts).

7.4 Accessing and use of Social Media and Blogging Web Sites

The county government will block access to social media sites for staff and stakeholders as a general rule. However, exceptions can be made for particular staff and stakeholders groups if it is deemed necessary for business or educational purposes

7.5 Reporting of incidents and making a complaint

Any alleged breach of this procedure should be reported in first instance to a staff Chief Officer's line manager in cases relating to staff.

In cases where breaches are considered serious, disciplinary action could ensue. Thirty parties seeking to make a complaint in relation to a breach of this procedure by staff or stakeholders(s), should avail of the county government's complaints procedure.

8.0 Social Media

8.1 Background

Through the responsible use of social media, county government of Busia is committed to safeguarding the confidentiality and reputation of stakeholders and staff, and the reputation of the county government.

For the purposes of this SOP, social media is defined as any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public or internal forum. This constantly changing area includes (but is not limited to):

- Online social forums such as Twitter; Facebook; Google+, LinkedIn, Instagram and Snapchat
- Blogs, videos and image-sharing websites such as YouTube and Flickr
- Messaging technologies such as Skype for Business
- Personal web space

These procedures should be followed in relation to any social media used to promote good practice; protect the county government and its staff and to promote the effective and innovative use of social media as part of official county government of Busia activities.

Although the county government will block access to social media sites for staff and stakeholders as a general rule, nothing is intended to restrict or inhibit activities involving social media in accordance with county government needs or legitimate county business or academic research that will benefit the county. Staff and stakeholders:-

- Should not use social media websites to criticise the county government, or any staff members, stakeholders or third parties.
- Should not use social media websites to abuse, harass staff members, stakeholders or any other third parties.
- All staff and stakeholders must remember not to post any comment, or image that would bring the county government into disrepute, or give cause for a third party to consider taking legal action.
- Must not place information pertaining to, or upload image(s) of county government staff or stakeholders to any web site without the prior consent being obtained from the staff and stakeholder member(s) in question.

8.2 Scope

This applies to all staff employed, or third parties engaged by, or on behalf of county government of Busia in relation to the use of social media for business, **whether it is in normal work time or not, on county government or personal computing facilities and whether posting on social media using personal or work related accounts.**

8.3 Breach of Procedure

Any breach of the procedures may lead to disciplinary action being taken against the employees involved in line with Human Resource Disciplinary Procedures.

The Marketing and ICT Infrastructure departments must be informed immediately of any breaches of Social Media procedures so that appropriate action can be taken to protect confidential information and limit damage to the reputation of county government of Busia.

8.4 Use of Social Media at Work

Staff may be required to make reasonable and appropriate use of social media as part of their work where this is an important part of how the county government communicates. Staff should be accurate, clear and transparent when creating or altering social media sources of information about county government of Busia.

Procedures for setting up social media for business purposes are set out in section 8.7. Staff must be aware at all times that, while contributing to the county government's social media activities, they are representing county government of Busia and should use the same safeguards as they would with any other form of communication.

Staff should keep their professional and personal lives separate when using social media. County government of Busia reserves the right to monitor internet usage as per the provisions of the relevant policies and laws.

When using social media for communicating county government of Busia business, staff must NOT:

- **Bring county government of Busia into disrepute**, for example by:
  - Presenting personal views as those of county government of Busia;
  - Criticising or arguing with citizens, clients, colleagues or rivals;
  - Making defamatory or libellous comments about individuals or other organisations or groups;
  - Posting images without the correct consent, or that are inappropriate, or links to inappropriate content;
  - Edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work as the source of the correction will be recorded as the county government of Busia IP address and will appear as if it comes from county government of Busia itself.

- **Breach confidentiality legislation or codes of conduct**, for example by:

- revealing confidential information owned by county government of Busia;
- giving away confidential information about an individual (such as a colleague, stakeholders, or customer contact) or organisation (such as a rival business); or
- discussing county government's internal workings (such as future business plans that have not been communicated to the public);

- **Breach copyright**, for example by:

  - using someone else's images or written content without permission; or
  - failing to give acknowledgement where permission has been given to reproduce something;

- **Breach data protection legislation**, for example by:

  - disclosing information about an individual without their consent;
  - allowing unauthorised access to the personal data held on a social media account on behalf of county government of Busia; or
  - processing personal data in such a way that would breach Data Protection principles;

- **Do anything that could be considered defamatory, discriminatory against, bullying or harassment of, any individual or organisation**, for example by:

  - attacking, insulting, abusing or defaming any stakeholders, their family members, staff, county government of Busia or other related professionals;
  - making offensive or derogatory comments relating to sex, gender reassignment; race (including nationality), disability, sexual orientation, religion or belief, pregnancy and maternity, marriage and civil partnerships, or age; or
  - Posting images that are discriminatory or offensive (or links to such content).

8.5 **Personal Use of Social Media**

County government of Busia does not permit personal use of social media during working hours without prior permission.

While they are not officially acting on behalf of county government of Busia, staff must be aware of the damage to the county government if they are recognised as being employed, or engaged by county government of Busia. Any communications that staff make in a personal capacity through social media must not bring county government of Busia into disrepute, breach confidentiality or copyright, breach data protection, or do anything which could be considered defamatory or discriminatory against any individual or organisation.

During personal use of social media, county government staff must NOT:

- Use county government email addresses and other official contact details for setting up, or communicating through, social media accounts.
- Identify themselves as county government of Busia employees.
- Publish photographs, videos or any other types of image of county government stakeholder on personal social media.
- Have contact with any county government of Busia stakeholder, unless that stakeholder is a family member or pre- existing personal friend.
- Have contact with any stakeholder's family member if that contact specifically relates to county government of Busia business, is likely to constitute a conflict of interest, or call into question the staff member's objectivity.

- Accept ‘friend requests’ from stakeholders; they should signpost stakeholders (during work time) to become ‘friends’ of one of the official county government of Busia social media sites.

- On leaving county government of Busia service, contact stakeholders via personal social media sites. Similarly, current county government staff must not contact stakeholders from any other establishment they were previously employed at by means of personal social media unless that stakeholder is a family member.

Staff should **apply caution** when inviting or accepting work colleagues to be ‘friends’ in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships if too much personal information is known in the work place.

Staff are strongly advised to ensure that they set the **privacy levels** of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff should keep their passwords confidential, change them often and be careful about what is posted online. It is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

8.6 Social Media Monitoring

The county government reserves the right to monitor employees’ use of social media on the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- Promote productivity and efficiency;
- Ensure the security of the system and its effective operation;
- Make sure there is no unauthorised use of the county government’s time;
- Ensure that inappropriate, restricted or blocked websites are not being accessed by employees
- Ensure there is no breach of confidentiality.

The county government reserves the right to restrict, deny or remove Internet access, or access to particular social media websites, to or from any employee.

8.7 Setting up Official County Government of Busia Social Media

There must be strong pedagogical or business reasons for creating official county government of Busia social media sites to communicate with stakeholders or others.

To apply to set up an official county government of Busia social media site:

- Complete the application form (Appendix 2) and submit to ICT Unit.
- If approved, the form at Appendix 3 must be completed and returned to ICT Unit.
- A 6 Month Review will be conducted of all presences (Appendix 4).
- Twitter and Facebook operational rules must be read and adhered to (Appendix 5) Available.

9.0 Network Management Procedure

9.1 Introduction

Purpose

The computer network is a fundamental service that provides the infrastructure to enable connectivity between all of the Subcounty's computing resources. It is vital that such a resource is properly controlled, maintained and managed.

The purpose of this procedure is to clearly delineate responsibility for all aspects of the computer network while at the same time allowing sufficient flexibility to ensure an efficient service can be delivered to the various county government Units.

Definitions:

- Remote Access Devices; Any equipment capable of establishing a physical network connection with a device or network that is not owned or operated by the county government.
- Network Components; Includes, but is not limited to: switches, routers, firewalls, interface converters, patch cables and data cabling, wall sockets, wireless access points, Remote Access Devices.
- End User Devices; PCs, Macs, Laptops, Macbooks, Servers, Workstations or other devices that are not performing the function of a Network Component.
- The county government's Computer Network; All of the county governments controlled Network Components that are directly or indirectly connected to the external interface.
- The ICT Support unit; The body responsible for all activities pertaining to the Computer Network.

Procedure

- The county government requires that only authorised persons shall manage and maintain the operation of the computer network.
- The ICT Support unit - has ownership of all Network Components comprising the Computer Network and will oversee procurement of all Network Components that are to be connected directly or indirectly to the Computer Network.

The ICT Support unit is responsible for the:

- Connection of any and all Network Components to the Computer Network. The ICT Support unit may, at its discretion, delegate specific activities to End User departments to support their activities as efficiently as possible.
- Configuration and management of all Network Components comprising the Computer Network.
- Management of all network based protocols (IP addresses, routing tables, DNS, DHCP, Routing protocols etc.).
- Management of all aspects of network security, traffic profiling, traffic prioritisation, authentication and control of access to the Computer Network.
- Performance monitoring and measurement exercises of the network.
- Management of radio frequency separation on all county government sites, for all wireless Network Components irrespective of usage.
- Management of the capital and revenue budget for the Computer Network.

- Disaster recovery of the network.
- The ICT Support unit will operate a Fault Reporting facility for the logging of all faults and problems with the Computer Network. All faults requiring the attention of the ICT Support unit must be logged. The ICT Support unit will work closely with nominated representatives of End User Departments to support the resolution of problems as efficiently as possible.
- Remote support tools will be used by ICT Support staff in order to provide end user support. Where possible, permission should be obtained from the end user before connection to the remote device takes place. Remote tools will not be used for "spying" unless there is due cause to suspect inappropriate use by an end user.
- There will be no monitoring or recording of the data content of packets traversing the Computer Network without the explicit permission of the ICT Support unit.
- Requests for VPN (Virtual Private Network) access to the county government Network for county government staff must be approved by the Departmental chief officer.
- The county government will provide remote access for staff and stakeholders to the county government Intranet. It is incumbent upon each remote user to ensure that their remote devices are protected by updated anti-malware software.
- Requests for remote access to the county government network or any county government ICT System by third parties must be addressed to the Head of ICT for approval.
- Third party access to the county government network must be via an agreed secure connection (e.g. VPN). The third party must inform the Head of ICT giving details of reason(s) for requiring access, the identity of the party or person accessing the network and the estimated duration of access.
- The third party shall inform the Head of ICT when the network access session is due to close. Confirmation of work carried out must be provided by the third party

9.1 Computer Accounts for Staff and Stakeholders

Staff and stakeholders will be given an account to log on to PCs/Macs for purposes of accessing e-mail, file storage, internet/intranet services.

Accounts will be set to expire upon the staff member leaving, or at the end of the activity end for a stakeholder. Accounts for staff on temporary and part time contracts will be set to expire at the same date as their contract end date.

10.0 Password Procedure

10.1 Introduction

Overview

Passwords are an important aspect of computer security. They are the front line protection for user's accounts. A poorly chosen password may result in the compromise of the county government's entire network. As such, all staff, stakeholder and contractors that have access to any computer system at any county government Centre are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

Purpose

The purpose of this procedure is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this procedure includes all staff, stakeholders and contractors who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any county government of Busia sites.

10.2 **Procedures**

- All system-level passwords (e.g. root, enable, Windows server administration, application administration accounts etc.) must be changed on at least a yearly basis.
- All user-level passwords must be changed at least every six months.
- Passwords should not be disclosed in emails, phone calls, questionnaires, or verbally via a third party.
- Where SNMP is used, the community strings must be defined as something other than the standard "public", "private" and "system" and must be different from the password used to log in interactively.
- All system-level and user-level passwords must conform to the guidelines described below.

10.2 **General Password Construction Guidelines**

Poor, weak passwords have the following characteristics:

- The password contains less than seven characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Your forename, surname, name of family, pets, friends, co-workers, course title etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - county government of Busia, Subcounty.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like 1234567, abcdefghi, qwertyuiop etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g. password1).

Strong passwords have the following characteristics:

- Contains both upper and lower case characters e.g. a-z, A-Z
- Have digits and punctuation characters as well as letters e.g. !@#£$%^&*()+-
- Must be at least 7 alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon etc.
- Passwords should never be written down or stored on-line. Attempts should be made to create passwords that are easy to remember. You could create a password on a song title, affirmation or other phrase. For example, the phrase might be: "This May Be One Way To Remember" could be a password of "TmB1w2R!"

10.3 Password Protection Standards

- Do not use the same password for county government of Busia accounts as for other non county government of Busia accounts such as personal e-mail accounts, Banking accounts, PIN numbers, or any other account. Where possible, don't use the same password for various county government of Busia systems. For example, select one password for the Agresso system and another password for the network log in.

- Do not share county government of Busia passwords with anyone, including administrative assistants or line managers. All passwords are to be treated as sensitive confidential county government of Busia information. It is not permissible to:-
    - Reveal the password over the telephone to anyone (apart from password resets - see 10.5).
    - Reveal a password in a single e-mail message (apart from password resets – see 10.5)
    - Reveal a password to a manager.
    - Talk about a password in front of others.
    - Hint at the format of a password.
    - Reveal a password on questionnaires or security forms.
    - Share a password with family members.
    - Reveal a password to co-workers while on holiday.
- If someone demands a password, refer them to this document or have them call someone in the ICT Support unit.
- Do not use the "Remember Password" feature of applications.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file or ANY computer system without encryption.
- Change passwords at least once every six months.

If you suspect your password has been compromised, report the incident to the ICT Support unit and change your password immediately.

10.4 Resetting Passwords

- All staff and stakeholders can reset their own passwords from a county government PC/Mac or from the county government Intranet remotely.
- All teaching staff can reset a stakeholder's password by using the Stakeholder Lockout Wizard which is available on the county government Intranet. Staff should not enter a stakeholder's password or request a stakeholder to disclose their password.
- All ICT Support Staff can reset any other county government password. In both cases, suitable ID must be produced before the password can be reset. Staff and stakeholders should not request their password to be changed via e-mail or telephone unless the ICT Support Staff member can have good assurance of authenticity of the person requesting. The minimum requirement for establishing authenticity is to obtain the stakeholder/staff number, name, department or name of another person in the same department, chief officer. Upon establishment of authenticity, the password can be disclosed as long as:
    - The password is broken into 2 parts and transmitted in two separate e-mails.
    - The password is supplied by the caller to the ICT Support staff and not vice-versa
    - The "User must change password at next login" attribute must be set by the ICT Staff member on the user account.

10.5 Enforcement

Password "cracking" or guessing may be performed on a periodic or random basis by ICT department staff. If a password is guessed or "cracked", the user will be required to change it.

Any member of staff or stakeholder found to have violated this procedure may be subject to appropriate disciplinary action.

11.0 ICT Security Controls and Incident Procedure

11.1 Introduction

This procedure outlines responsibilities, structures, controls and the process for reporting ICT systems security incidents. It applies primarily to staff of the CGB. However, all users of county government information systems are expected to abide by this and all procedures related to ICT systems security.

With increasing reliance on electronic information comes a corresponding concern for the security of that information, particularly with mobile technologies such as wireless and 4G.

Since neither the systems, technologies nor those who operate them can ever be totally reliable, the county government must be able to react promptly and appropriately to any security incident, and to restore its information systems to their normal operational state in an acceptable period of time. One of the most fundamental aspects of information security is an information security procedure which amongst other things, defines responsibilities for information security and identifies the needs for security controls.

11.2 Requirements for Security Controls

A number of security controls are in place to permit the proper management of information security. Key controls are as follows:

ICT Management Control

The role of the Security Management Group (SMG) is the principal management structure for overseeing key aspects of corporate ICT systems security. This group will have responsibility for:

- Policy and guideline formulation on security.
- Provision of guidance and direction to the county government's Governing Body and county government Management team on security issues.
- Ensuring that there is management support for security initiatives.
- Managing security incidents.
- Co-ordinating implementation of corporate security measures.
- Initiate security audits and ICT risk assessments.
- Identifying risks to ICT systems and services and ensuring that they are recorded on the county government's risk register for presentation to the Risk Management Group.

The group will play a key part in informing and advising all users of ICT systems in the county government of major security policy decisions and plans for implementation. Should a security incident occur, the SMG will have authority to scrutinize the results of log file monitoring.

System Management Controls

Data Owners (System Managers), for all major county government systems, will have primary responsibility for ensuring that:

- Appropriate security measures are in place to safeguard services and data.
- Key stakeholders are informed and abide by security policies and procedures for each system.

- Ensure that breaches in security are reported to the Security Management Group.

System Controls

Each system itself will have in-built or configured security controls to guarantee the integrity of data and services. Controls include:

- Access levels (See also Access Control Procedure)
- Password controls. (See also Password Procedure
- Authentication measures (where appropriate).
- Data encryption (where appropriate).
- Backup.(See also Data Management Procedure)

Physical Controls

Controls such as secured areas for location of key ICT items will be provided. Doors to any ICT device will be locked whilst the area is unattended.

Authorised personnel only will be permitted only to restricted areas such as communication and server rooms.

11.2 Security - Good Practice Guidelines

Security Good Practice – DOs

- Lock workstations whilst left unattended.
- Report suspicious behaviour or persons acting suspiciously
- Bring laptops in weekly to connect to the county government network for anti-malware and Windows updates
- Check that your PC/laptop has up-to-date anti-malware software installed.
- Change your password when prompted to do so.

Security Good Practice - DON'T s

- Disclose your password to anyone.
- Leave rooms unlocked that contain ICT equipment.
- Use someone else's password.
- Open unexpected e-mail message attachments
- Accept as genuine all e-mail content.
- Spread chain mail (e-mail that you are invited to pass on to others).
- Leave passwords written for viewing by others.
- Use names of family members as passwords.
- Supply personal or business information to any third party unless authorised to do so.
- Store any personal or business data on local drives of PCs, Macs, MacBooks or laptops unless the drives are encrypted
- Attach any device to the county government network unless authorised to do so.

11.3 Procedure for reporting a security incident or security vulnerability

- Contact the appropriate Data Owner immediately.
- In conjunction with the Data Owner, complete an incident report
- Remedial action to be taken by the Data Owner (where possible) and SMG to be informed.
- In such cases where immediate remedial action cannot be taken to fully address the issue, a contingency arrangement must be implemented by the Data Owner in agreement with the Head of ICT to reduce the risk of a further security incident occurring. This arrangement will be in force until a permanent solution is implemented.

11.4 Responsibilities for Information Security

Whilst all users of county government information systems have a responsibility to some degree of ensuring that security is not compromised, overall management responsibility for security of county government ICT Systems rests with the Head of ICT and the Security Management Group. Each Data Owner will have specific management responsibilities for their respective ICT information systems. Their key responsibilities are:

- Remove user accounts of users that no longer require access to the data or system.
- Ensure passwords for users are changed regularly.
- Conduct security audits.
- Ensure backups have taken place.
- Conduct regular risk assessments.
- Retain accurate system administration information and store such information securely – (i.e. user names, access granted).
- Report unusual system activity (poor performance, unreliable or unexpected data results).

11.5 Links with other bodies

The county government will retain links with other bodies with regards to information security. Internally, the SMG will liaise closely with Chief Officers in terms of identifying significant ICT-related risks

11.6 Responsibility

IMT, through the SMG, will be responsible for ensuring that all ICT Systems users are:

- Made aware of the content contained in the security policy and associated policies or procedures.
- Ensure that all staff receive training on the procedure and general security.
- Ensure that policy and procedure revisions and updates are communicated to all users.

12.0 Software Licensing Management Procedure

12.1 Introduction

The county government is committed to ensuring that all commercial software applications installed on any of its ICT equipment items are appropriately licensed in accordance with numbers of users who require access. This procedure document outlines the main procedures and controls in place to ensure that licensing regulations are not violated.

12.2 Access

In order to prevent installation of unlicensed software, only ICT Support staff have the necessary access to install software.

Access is granted to the following:

- PCs, laptops, Macs and MacBooks – all ICT Support Staff – (depending upon the method – see Section 12.3. Method of Installation**)**.
- Servers – Senior ICT Support staff only.

- Apple Macs – The technical support staff who work for the department of ICT.

12.3 Method of Installation

There are two main methods of software installation:

- Deployment – Only ICT Support staff are permitted to deploy or authorise deployment of packaged software.
- Manual Installation – Only ICT Support Staff are permitted to install software manually. Regardless of method type. Installations can only take place if sufficient software licences have been procured. Approval for installation must be obtained from the Head of ICT.

(Software Installation Procedure provides details for ICT Support staff on installation of software)

12.4 Authorisation

The procedure for authorising software installation is as follows:

- Request for software installation to be addressed to the Head of department.
- If approval in previous step is granted, then the request is to be forwarded to Head of ICT.
- Installation authorisation to be granted by Head of ICT to appropriate ICT technical staff.

12.5 Control

All staff and stakeholders (other than groupings stated above in Section 12.2) do not have the necessary permissions to install software on PCs and laptops.

12.6 Procurement and Recording

Procurement of application software must be carried out by the Head of ICT.

13.0 Data Management Procedure

13.1 Introduction

An influx of new technologies, greater dependence on electronic data and changing working practices such as hot-desking, have contributed to make it more difficult for an organisation to manage data. The purpose of the procedure is to provide guidance on managing corporate data within the county government. The procedure will in most part apply to county government staff but will also have an impact on stakeholders on terms of management related data.

13.2 Definitions of data types

"Data" will include any type of information stored on any electronic storage medium, including files, documents, e-mail, database records. Broadly speaking, data will be classified into two main categories:-

- Personal, Confidential and Sensitive data
- Other data

Personal, Confidential and Sensitive data

'Personal' can be defined as:-

- Any information containing names **and including** any, or all of the following:- Dates of birth, addresses, postcodes, financial details such as banking details, medical details or histories and photographic images.

'Confidential' can be defined as:

- Any business information that is classified as "confidential"
- Any information that would offer competitive advantage to other county governments, or competitors
- Any information that could mean loss of business, revenue or reputation to the county government of Busia should that information be available outside of the county government domain
- Any security information such as system passwords, user account details.

'Sensitive' can be defined as:

- Any information relating to medical, financial, criminal or sexual orientation circumstances.

Other data

'Other data' includes any other stored data which does not fall into the 'Confidential', 'Sensitive' and 'Personal' category.

13.3 **Management of Electronic Data – Both Classifications**

Storage and Transmission of Data

- Source data must be stored securely on county government -secured storage media such as shared drives on county government of Busia servers or on the county government of Busia-provisioned Office 365 OneDrive.
- Source or copy data of personal, sensitive or confidential type must not be stored on any external hosted service such as Dropbox, Google Docs or Evernote or any other similar storage service. The only approved external hosted storage service is Office 365 OneDrive. (This has the Government G-Cloud approval for storage for personal, confidential and sensitive information).
- Copies of 'other data' can be taken to facilitate remote, or off-site working (e.g. lesson material), for use in a facility with no internet connection.

- Copies of source data regarded as personal, sensitive or confidential must only be taken and transported by portable media as long as:
    - Approval has been sought from Chief Officer of the department.
    - That the method of transportation is deemed secure. Personal, sensitive or confidential data must be transported in encrypted media such as encrypted USB pens, or on encrypted hard drives, or on county government -owned laptops that have encrypted hard drives, or any other approved secure media.
    - Great care is taken not to lose or mislay the storage device.
- Secure means of transmission of data must be used (e.g. transmission via secure internet connection with county government approved encryption algorithm). Data must not be transmitted by unencrypted e-mail messages, instant messaging or any other insecure means or media.

- It is not permissible to store personal, sensitive or confidential data on:
    - Personally owned devices such as PCs, laptops, MacBooks, tablets or mobile phones
    - Any storage medium, (personal or county government provided), if that has not been encrypted. This includes memory sticks, hard drives, camera cards, DVDs and any other storage media

Retention of data storage

- The county government will retain data records in accordance with statutory obligations.
- The county government will remove mailboxes and data created by stakeholders.
- Staff who are leaving county government of Busia employment are advised to clear out their personal storage and mailboxes before their last day of employment. Staff should pass on information that could still be required by the county government to their Chief Officer. This could include reports, financial or business information.
- Upon receipt of notification from the Human Resources department of staff having ceased employment, staff network login accounts will be disabled. All data and mailbox contents stored against a disabled account will be deleted after a three month period.
- The county government will not be responsible for loss of data created by staff members or stakeholder upon their ceasing their employment or contractual period with the County.

Backup

- The county government will endeavour to backup and store on and off-site all corporate data. The county government backup procedures must be adhered to in performing data backups.
- Where possible data records, files and documents should be updated on-line or directly to network drives.
- Copies of data taken and updated by staff/stakeholders must be uploaded to the appropriate storage area to ensure that the revised content is backed up (e.g. updating of documents or folders must be uploaded to the area where source information was stored, or if new copy was created, it must be uploaded to the appropriate storage area

that the author has access to. Version control measures must be employed.

Data Recovery and Restoration

In the event of data loss or corruption from the county government file storage, the following steps can be taken to restore:

- By utilising Shadow Copy. If a folder or file has been lost or corrupted it can be restored by right-clicking the file or folder in question and then selecting the "Restore from Previous Version" option.
- By contacting the ICT Support Section or Data Owner in order to restore from the last disk backup

Remote Access

Accessing county government information systems from a remote location such as a place of employment or from home is permitted as long as:

- The PC/laptop/AppleMac/tablet used is secured with the latest anti-malware software and that virus definitions are continually kept updated.
- Passwords are not disclosed to third parties and that third parties are not permitted to access county government services using the staff or stakeholders member's account.
- Staff/stakeholders log out on completion of the access to county government ICT systems.

13.4 **Security**

All corporate data must be stored on secured county government servers with the appropriate authorisation for access granted by the relevant System Manager.

User logins and passwords

Each user of a county government system must be allocated a user account and password. Accounts can only be setup upon notification from Human Resources Department that all appropriate checks and controls have been completed (this includes signing of Acceptable Use Policy). Passwords must comply with the county government password procedure

Version Control

Manipulation of copied data incurs risk of partially updated copies of the source documents or files. On-line editing reduces greatly the risk of multiple copies of partially edited or out- dated documents. However, in instances where on-line editing isn't possible, each edited document should have a date of revision and author name added to the document footer.

Malware Prevention

All county government servers and desktops will be updated with the latest anti-malware definitions. Only devices with latest anti-malware software are permitted to be used for processing of county government data.

13.5 **Asset and Inventory Management**

All items used by staff (asset and inventory) such as PCs, laptops, MacBooks, Macs and servers must be data wiped prior to disposal. Data wiping includes removal of all data and software from the device(s).

13.6 **Access to Data**

Departmental Shared Drives (Staff Resources (S Drive) and Team Sites
Requests for access to above should be made via the Fault/Request App and ought to be accompanied with approval from the relevant Chief Officer, via e-mail message, indicating the name(s) of staff members and the level of access to be granted (i.e. read access, read and write access).
Requests for access to Staff Resources folders will be processed by the.

Requests to access another staff member's personal drive, OneDrive or mailbox.
Each staff member / stakeholder have their own personal drives and mailboxes. Only that individual has the right to access their own personal drive and mailbox. The following are the only exceptions in terms of other rights to access:-

- There is suspicion that inappropriate material is being stored. In such cases, either the relevant Chief Officer will consult with the Head of ICT as regards arranging to access the drive/mailbox. The access must be witnessed by the relevant Chief Officer and by Head of ICT or a senior member of the ICTUnit.

- A staff member is on extended period of absence due to illness or annual leave. Access to the staff drive/mailbox will be granted in urgent cases only if the request is made by the relevant Chief Officer indicating the reasons for requiring access to the Head of ICT and only if the staff member in question has given prior approval in writing (e-mail will suffice) to the Chief Officer and copied to Head of ICT. As stated above, the access must be witnessed by Head of ICT, or a senior member of the ICT department. The access will only be for a duration long enough to obtain the necessary information and whilst witnessed as stated above. Browsing of the personal drive or mailbox for information other than the required information is forbidden. Once the required information has been located, the access will be removed. The required information is not to be copied or forwarded on, unless the staff member has authorised that.

- If for various reasons, the matter is regarded as most urgent and the staff member's approval cannot be obtained, the matter must be referred to the Head Human Resources for deliberation.

- Members of the ICT section are not permitted to request access, or to access any other staff member's personal drive or mailbox without the above process being followed.

Requests to access personal data on any information system or store
Access requests must be made to the System Manager and Data Owner and must comply with procedures devised for compliance with data protection.

13.7 **Discovery of inappropriate data, files, images**

Discovery of data, images regarded as inappropriate includes the following:-

- Copyright protected files or images
- Images regarded as pornographic, obscene
- Unlicensed software

- Software or utilities regarded as hacking, sniffing, or that can be used in any way to circumvent network or system controls or security.

(The above listing is not to be regarded as definitive)

Discovery of any above must be reported immediately to the ICT Support Section so that removal of the items can be arranged. However, discovery of any material which has constituted a criminal offence, or could form part of a criminal investigation must be reported to the Chief Officer in charge of ICT Unit.

13.8 Disclosure of Information

It is not permissible for any county government information, or any information contained in any county government information system to be disclosed for purposes of offering competitive advantage to any third party. It is also not permissible for any staff member to use any information to further any independent or private business venture.

13.9 Good Practice Guide on Data Management and ICT Security

County government of Busia must ensure that personal data of staff and stakeholderss is treated with appropriate security measures by all who handle it.

Loss of personal data has substantial risk of causing harm/inconvenience to the data subject and reputational damage to the county government of Busia.

PASSWORD SECURITY

ALWAYS…..
• Create strong passwords which are easy for you to remember and impossible for someone else to guess. • Strong passwords should be at least 7 characters long with a combination of letters, numbers upper/lower case and even symbols such as @*!£&$ • Change password at regular intervals

NEVER….
• Use birthdays, addresses, family names, pet names etc…. • Disclose your password to anyone, even other members of staff. • Write your password down or save it on a word document. • Select 'yes' if a system asks if you want it to remember your password. • Disclose your password in response to an email purporting to be from the IT department. They will NEVER ask for your password!

DATA / INFORMATION SECURITY

ALWAYS…..

- Store personal/confidential/sensitive information on secure county government storage systems i.e. teamsites/network drives.
- Lock your PC/Mac whilst unattended – 'Ctrl + Alt + Del +"Lock this computer".
- Lock classrooms and office doors once everyone has left.
- Ensure your personally owned device (PC, mac, tablet, laptop/MacBook) is password protected and has up to date anti-malware software installed.
- Have at least a lock password on mobile phones with access to email.
- Report any suspicious activity to the ICT department e.g. people loitering around equipment.
- Bring county government provided laptops/MacBook on a weekly basis into the county government and ensure that they are connected to the county government of Busia network for application of essential security updates.

NEVER….

- Store personal/confidential/sensitive information on an unsecured mobile device such as a USB pen, personal or third party PC, Mac, laptop, MacBook or external hard drives.
- Store personal/confidential/sensitive information on a personal mobile phone.
- Store personal/confidential/sensitive information on a third party storage facility such as Google Docs, Dropbox, Evernote – we cannot guarantee their security. The exception to this will be Office 365 OneDrive.
- Use your personal email account for county government of Busia related business - we cannot guarantee their security.
- Allow anyone to use your PC/Mac, MacBook, laptop or tablet whilst you are logged in – you are responsible for processing carried out under your name.
- Provide personal details of yourself or others to unauthorised third parties.
- Respond to web links requesting personal details of yourself or others.
- Do not have liquids close to your device in case of spillage.

'CGB' HANDHELD AND PORT ABLE ELECTRONIC STORAGE DEVICE SECURITY (E.G MOBILES, LAPTOPS, MEMORY STICKS ETC)

ALWAYS…..

- Guard your mobile device (i.e. mobile, laptop, MacBook, tablet) as you would do with your purse, wallet, passport.
- Wipe all data from the device before disposing of it.
- Report any loss of mobile device to the IT department and change your CGB password as soon as possible.
- Turn off Bluetooth to prevent data transfer.

NEVER….

- Leave your device in your car where is it visible to passers-by.

PHOTOCOPIERS/SCANNERS

ALWAYS…..

- Store printouts securely e.g. a lockable drawer.
- Shred hardcopy personal data which is no longer of use or dispose of in a confidential waste bag.

NEVER….
• Leave the original copy in the photocopier/scanner – always remove it once copying is complete. • Leave copies of personal data where it can be accessed or viewed by other people e.g. staff rooms, unmanned office desks, reception areas.

REMEMBER:

It is the responsibility of all staff and third parties authorised to access the county government's personal data sets to ensure that those data, whether held electronically or manually, are kept securely and not disclosed unlawfully, in accordance with the county government's. Unauthorised disclosure or data loss will usually be treated as a disciplinary matter, and could be considered as constituting gross misconduct with, in some cases, access to facilities withdrawn or even criminal prosecution.

14.0 Remote Access and Mobile Computing Procedures (including Bring Your Own Device)

14.1 Introduction

Technological advancements in mobile computing and changes in working practice have heralded an age which encourages access to information almost at any time and at any place. Whilst the new found flexibility is welcomed by many employees and internet users, there are many more risks to be addressed by ICT network managers in terms of ensuring secure access to the corporate ICT systems, especially with the proliferation of tablet devices and smart mobile phones. Employees, guests and stakeholders seek access to corporate and business information on personally owned devices rather than using the corporately owned computing infrastructure.

The purpose of the procedure is to provide guidance to county government of Busia staff and stakeholders on acceptable use of portable media and to provide guidance on accessing county government network and systems from remote locations

14.2 Mobile Computing

Categories of portable devices include:-

- USB memory sticks
- Tablet computers
- Mobile phones with messaging capability and data storage
- Laptops, Macbooks
- Other media such as DVDs, portable hard drives, MP3/MP4 players, camera memory cards

(The above is not a prescriptive list)

Working with portable media and devices

The following guidelines should be adhered to:

- Personal, sensitive or confidential information should not be stored on any portable device unless that device supports encryption and has been approved for use by a county government authority such as Head of ICT.
- Only encrypted devices should be used for storage of personal or confidential data.
- Persons using portable media must ensure that devices are not left unattended in public places.
- Portable devices must be adequately secured (e.g. laptops are not left logged on).

- Loss of portable devices must be immediately reported to the staff member's Unit Head or Head of ICT. If it has been established that personal or confidential data has been stored on the stolen device, the incident will be escalated to the Security Management Group (SMG).
- CGB owned laptops must be connected to the county government network at least once per week for anti-malware, application and operating system updates.
- County government of Busia owned laptops must have data encryption enabled on the local hard drive. (This is dependent upon hardware capability to support encryption method).
- county government of Busia provided mobile phones with messaging capability must have a pin number or password set on the handset.

Bringing in Your Own Device (BYOD)

Non county government -owned computing devices (laptops, tablets, MacBooks) can be used within the county government as long as critical updates have been applied (e.g. Anti-malware, operating system and application). Connection to the Busia county wireless network is permitted. However, staff or stakeholders who chose to access the wireless network through their own devices do so at their own risk. The county government will not be responsible for any damage, data loss or corruption during or after connection to the wireless network.

14.3 Data Control and Authority

As data controller, CGB must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. Staff are required to store CGB information and data securely. This applies equally to information held on the CGB systems and to information held on an employee's own device.

Conditions

The CGB permits access to the following ICT services with personally owned or third party devices as long as:

- Internet/intranet access – the device, (PC, laptop, MacBook or tablet), has up-to-date anti-malware software, critical operating system and application updates installed. Access to the CGB network will be via the CGB or ICT wireless network. Staff or stakeholder who chose to access the wireless network through their own devices do so at their own risk. The CGBe will not be responsible for any damage, data loss or corruption during or after connection to the wireless network.
- No data classified as personal, sensitive or confidential is stored on them. Any information deemed personal, sensitive or confidential must be deleted or removed immediately. In the context of e-mail messages, the Deleted Items folder must also be emptied.
- Staff members must familiarise themselves with the device sufficiently in order to keep the data secure. In practice, this means:

- o preventing theft and loss of data,
- o where appropriate keeping information confidential and
- o maintaining the integrity of data and information.

Staff members should:

- Delete sensitive, confidential or commercial emails once finished with them.
- Delete copies of attachments to emails such as spread sheets and data sets on mobile devices once finished with them.
- Limit the number of emails and other information that are synced to their device.

Loss or Theft

In the event of a loss or theft, the password to all CGB systems accessed from the devices should be changed (and it is recommended this is done for any other services that have been accessed via that device, e.g. online banks, etc.).

Any loss or theft of a device should be reported promptly to the CGB ICT Department. It may be necessary to invoke a "remote wipe" of the device. It is recognised that remote wiping of data may result in the loss of the employee's personal information held on the device. A "remote wipe" will not be carried out without consultation with the device owner.

Security and Integrity of the Device

Staff are required to play their part in maintaining a safe working environment and in terms of BYOD, this means keeping software up to date and avoiding content that threatens the integrity and security of their device(s), the CGB systems and the devices of other staff or stakeholders. The CGB will enforce a security policy on each mobile phone that is granted access to e-mail. This will force the setting of a pin number/password. The phone will automatically lock after one minute of inactivity.

Monitoring of User Owned devices

In exceptional circumstances, the CGB may require to access county government data and information stored on your personal device. In those circumstances, every effort will be made to ensure that the CGB does not access the private information of the individual. CGB data and information can only be stored and processed on personally owned devices under acceptance of these conditions.

14.3 **Remote Computing**

"Remote Computing" for the purposes of this procedure, can be defined as accessing any CGB system from a device in a location that is not part of, or directly connected to the CGB data network. It includes accessing the CGB network from home or external workplaces.

Working from a remote location

The CGBe will provide a secure connection for remote access such as SSL (Secure Sockets Layer), VPN (Virtual Private Network), or other secure method. The following guidelines should be adhered to when working from a remote location in terms of accessing CGB ICT systems:-

- Devices used from a remote location must have updated anti-malware software installed.
- Only CGBe staff will be permitted to access CGB ICT systems from remote locations. Third parties are not permitted to access CGB systems from a CGB staff or stakeholder member's user account. It is incumbent upon staff and stakeholder to ensure that they do not disclose password details to any third party and that they ensure that they have logged off from the CGB system and remote device before leaving the same device.

- Any files to be copied to a CGB storage area must be malware checked in first instance by the person wishing to copy or upload the file. Infected files must not be copied.
- It is not permitted to copy large files from a remote location to a CGB server unless prior consent from the ICT Support section has been granted. File compression utilities should be used on any file over 20MB (megabytes) in size.

14.4 General Guidelines

Version Control

Due care must be taken when working remotely or with copies of source documents on portable media that appropriate version control takes place. It is recommended that copy documents have a version number appended to the file name (e.g. mobilecomptungVer1.doc). Each document should also have a date of revision, author and name added to the document footer. The source document should only be overwritten with the approved version. Approval should be sought from Departmental Heads in situations where documents are to be copied to shared departmental drives.

Copy documents should be deleted once the approved document has been uploaded to the appropriate storage area.

Use of Third Party Devices

Users of third party devices requiring networking connectivity other than via the wireless network, must seek prior permission from the ICT Support Department.

Wireless networking

The CGB does provide comprehensive wireless access across all subcounties. The CGB or ICT wireless network service is available to staff and stakeholder to use on CGB- provided or on personally owned devices. Authentication is required via a valid staff/stakeholder e-mail address and password. Each laptop ought to have the latest anti-malware software definitions installed and should have the latest operating system (Windows/OSX) updates applied.

It is not permissible for anyone to connect any wireless access point to the CGB network or indeed to connect any device to the CGB wired network. ICT personnel only are permitted to carry out such tasks.

15.0 Communication Plan

This Procedure will be uploaded to the CGB intranet and referred to in staff induction and training.

16.0 Review

Procedures associated with ICT security will be reviewed at least every 12 months. Additional reviews and updates will take place inside that timeframe if

new systems are implemented and/or if significant infrastructural changes take place (e.g. new campuses connected to the network, server installations and refurbishments).