ICT Acceptable Use Policy

Department: Centum Business Solutions IT

Effective Date: 1st August 2015

Version: 3.0

Document control:

This document is a version controlled document. All changes are recorded in the following version control table:

Version	Details of changes/management	Date
1.0	Initial Draft	22/7/2015
2.0	Revised and Approved	12/3/2016
3.0	Revised and Approved	23/2/2017

TABLE OF CONTENTS

1.0 ICT ACCEPTABLE POLICY

1.1 INTRODUCTION

The ICT Acceptable Use Policy describes the position of Centum Investment regarding how ICT will be used to achieve desired goals.

The policy seeks to:

- Provide a framework for operating in a uniform, predictable manner and to ensure that ICT truly reflects priorities and is in consonance with the objectives and aspirations of Centum
- Provide a basis for safeguarding Centum's Information, Brand image and ensuring conformance to legislative requirements.

1.2 POLICY FRAMEWORK

The Acceptable Use Policy is divided into;

Policy	Description
Email Use Policy	This policy covers appropriate use of any email sent from Centum. It covers email management,
ICT Security Policy	This top-level information security policy is a key component of Centum overall information security management framework. The objective is to preserve confidentiality, integrity and availability of Centum's IS.
Information Classification & Management	The purpose of this policy is to support the classification of information enabling the protection of Centum's data, in terms of confidentiality, integrity, and availability. It is also intended to provide guidance on the file naming scheme for the company.
Internet Use Policy	The policy sets out the responsibility of individuals using the service in order to maximize the benefits of Internet access whilst minimizing the risks.
ICT Acquisition & Disposal	This policy defines the process for acquisition of ICT infrastructure and the approved software and hardware standards.

Information Management Policy	The purpose of this policy is to provide guidance and direction on the creation and management of information and records and to clarify staff responsibilities. Centum is committed to establishing and maintaining information and records management practices that meet its business needs, accountability requirements and stakeholder expectations.

The details of each policy group follows;

2.0 EMAIL USAGE POLICY

2.1 INTRODUCTION

- This policy sets out the general rules for the use of Centum's e-mail system, together with specific protocols and guidance concerning the data protection implications.
- The Company's e-mail systems are coordinated and managed by Information and Communication Technology (ICT).No other e-mail system (server or client) is recognised by or supported within Centum.
- Well managed use of e-mail and other electronic information systems will, in accordance with the Company's Information Strategy, reduce the need for paper-based communication.
- It is a condition of use of IT and e-mail facilities provided by the Centum, by a member of staff or other authorised person that the user agrees to be bound by the relevant Policies and Regulations.

2.2 USE OF E-MAIL

- The e-mail systems are centum property and the Centum reserves the right to monitor and to access any e-mail messages.
- The use of e-mail for incidental and occasional personal purposes is permitted for convenience but should not be used for private confidential correspondence. Such use must not directly or indirectly interfere with the Company's systems or burden Centum with any incremental costs.
- All users are responsible for ensuring that their e-mail usage is within the regulations, is ethical and lawful.
- The sending of text or images that contain material of an offensive, indecent or obscene nature is prohibited.
- Access to the centum e-mail systems for staff is available via VPN, HTTPs and Blackberry. Provided the appropriate security guidelines are followed (see IT Security Policy, document).
- E-mail may be an inappropriate medium for the transmission of very sensitive or confidential information. If in doubt, alternative methods of communication should be employed, or advice sought.
- Users of e-mail should be aware of formal requirements and good practice in the use of e-mail as set out in the sections below.

- E-mail may be used for any legal activity in furtherance of the aims or policies of Centum, subject to the conditions listed below. The following specific uses are excluded:
    - Any use that violates Centum policies, standards as set out in HR Manual or Brand Guideline.
    - Any use that brings Centum into disrepute;
    - The transmission of e-mails with or without attachments that are known to contain viruses or other harmful software;
    - The use of another individual's e-mail account by using that individual's identity (i.e. the individual's username/password details);
    - The use of e-mail that could result in the inadvertent commitment of Centum to a contract or agreement if it appears to the other party that he/she has authority to do so;
    - The creation of anonymous messages. All e-mails must be attributable to a named sender;
    - Impersonation or misrepresentation of another individual;
    - Alterations of source or destination address information;
    - The use of external e-mail accounts (e.g. yahoo, gmail) for Centum purposes: this is to comply with security, sender authorisation and data protection issues. This includes auto-forwarding of Centum e-mail to external accounts;
    - The use of e-mail for personal reasons to promote or denigrate companies or organisations, or defame other employees;
    - The use of bulk e-mails, including excessive use of mailing lists, which is unrelated to the legitimate Investment activities of Centum and is likely to cause offence or inconvenience to those receiving it;
    - The use of Centum e-mail for any commercial activity or monetary gain;
    - Sending copies of documents in breach of copyright laws and Intellectual property rights;
    - The use of e-mail to harass or intimidate others or to interfere with the ability of others to conduct Centum business.
- ICT will provide (upon request and authorisation from line Manager) a method that allows staff to forward their Centum e-mail to another e-mail address but having e-mail redirected does not absolve the staff from the responsibilities associated with communication sent to his or her official

Centum e-mail address. Staff must correspond with business partners via the Centum e-mail system only and not with any external e-mail address.

2.3 MISUSE OF E-MAILS

- Penalties for misuse of e-mail will depend on the seriousness of the offence, and will be in accordance with current HR Manual

2.4 CODE OF PRACTICE FOR ALL E-MAIL USERS

- Users should adhere to the following guidelines for appropriate use:
    - Check your e-mail regularly
    - Email communication must be in line with the brand guidelines.
    - Be polite. Messages sent by e-mail can often seem abrupt, even when this is not the intention. Use professional courtesy and discretion. The use of all upper-case text in either the subject or the body of an e-mail should also be avoided as this is deemed to be the e-mail equivalent of shouting;
    - Before you send an e-mail, read it through to make sure it really does say what you want it to say;
    - Do not say anything in an e-mail that you would not be prepared to say to someone face to face;
    - Do not reply "With History" if it is not necessary especially if it incorporates a large attachment.
    - Use 'reply all' and distribution lists with caution in order to keep the number of messages to a minimum and reduce the risk of sending messages to the wrong people;
    - Messages should be addressed to those from whom an action or response is expected, "cc" or "bcc" should be used for other recipients for whom the message is for information only;
    - Respect peoples' privacy and consider this aspect before forwarding messages;
    - Delete unwanted or unnecessary e-mail. It is the user's responsibility to manage their e-mail folders and keep within reasonable limits. ICT can give advice and assistance if required;
    - Unsolicited e-mail, especially with an attachment, may contain a virus or other harmful software. If in doubt, delete the e-mail or contact ICT
    - Do not try to carry out confidential or sensitive tasks or express controversial views via e-mail;

- Enter a meaningful title in the 'subject' field at the top of the e-mail to help the reader anticipate the content correctly. Try to keep to one subject per message to help avoiding unnecessary confusion;
- Don't use all or part of someone else's message without acknowledgement. Don't edit someone else's message without making it clear what the changes are that you have made. Don't distribute other people's messages without permission;
- Avoid subscribing to unnecessary mailing lists. Unsubscribe from mailing lists when they are no longer required;
- Do not forward e-mail "chain letters". These are e-mails which either ask you to forward them on to all your friends (or to everyone you know) or which state that something bad will happen if you do not forward them. E-mails of this type, which are warning about something (e.g. computer viruses), are almost certainly hoaxes as well.

2.5 CAUTIONARY NOTES

- The nature of e-mail is such that total confidentiality cannot be guaranteed and users should be aware of the following points about e-mail use:
  - Copies of e-mail may exist on a back-up copy or a remote system even after the author or recipient has deleted the message;
  - E-mail may be forwarded by any recipient without the author's consent: it may not have been the author's intention that the mail should be forwarded.
  - A forwarded message may be a modified version of the original;
  - It is possible for the author or sender of an e-mail to disguise or alter their identity.
  - Organizations outside Centum may have different e-mail policies. Some consider it the property of the organization, subject to examination, copying or forwarding. Be aware of this possibility when sending e-mail;
  - A reply to a personal message sent via a 'listserver' or electronic bulletin board may be inadvertently distributed to all subscribers to the list;
  - Usernames and passwords should not be disclosed to others. This could result in security breaches and other people using your e-mail

account to send unauthorised messages. Suspected security breaches should be reported to ICT at once;

- Once a message is sent, there is no way to retrieve it. Check carefully that messages are addressed to the correct recipient(s) before sending.

2.6 AUDITING

- ICT does not routinely monitor or access e-mail. However, all e-mails arriving at Centum servers are automatically scanned for viruses and for "spam" content i.e. whether they match unsolicited, nuisance, e-mails previously sent to Centum: all such e-mails are blocked. However, filtering/virus-scanning can never be 100% effective so any unsolicited e-mails and attachments should always be treated with caution. Similarly, an e-mail may be incorrectly marked as infected or "spam" and become unnecessarily blocked.
- ICT reserves the right of access to users' e-mail and audit logs on both the client workstation as well as the servers for legitimate purposes, such as investigation of complaints of misuse. Contents and audit logs for both sent and received e-mail may be inspected (including personal e-mail) at any time without notice.
- ICT will endeavour to maintain privacy of e-mail. However, there may be special cases where it is essential that e-mail messages are accessed. In these instances, on the request of a Line Manager,ICT may locate and make available e-mail messages for access by a nominated member of staff. The owner of the mailbox will be notified in due course.
- ICT Manager may necessarily have access to the contents of e-mail messages in the course of system administration. Any knowledge thus obtained will not be communicated to others, unless required for system administration.
- ICT reserves the right to take special actions in administering e-mail if this is essential to preserve the integrity or functionality of the system. This may include the deletion of e-mail.

2.7 RETENTION

- ICT will put in place an automatic centralised system to archive e-mails. This enables the tracking and retrieval of previous e-mails in respect of correspondence that would be significant in an internal or external matter
- The e-mails are simply stored as part of an archiving system. Centum may use personal data contained within e-mails for particular purposes when its purpose is set out or clearly implied by the nature of the e-mails.
- E-mails will be archived for a period of 3 years.

2.8 DELETION AND ARCHIVING

- E-mail messages are archived along with other files in accordance with existing ICT operational procedures so messages deleted by the user may still be held in archives. However, archiving of e-mail messages is not guaranteed so users should make their own copies of essential messages.

2.9 SECURITY – OPENING AND CLOSING ACCOUNTS

- E-mail accounts for staff are set up by ICT on receipt of a request from Human Resources Manager. Associated passwords are issued directly to the end user
- Staff accounts are deleted on receipt of a request from Human Resources Manager.
- Before leaving employment at Centum, staff should unsubscribe from any e-mail lists they have subscribed to.
- Following the departure of a member of staff from the Centum, their e-mail account will be closed for access by them and deleted after a period of 8 weeks. Centum management may request access to be given to the closed mailbox by another member of staff for this duration.

2.10 DISCLAIMER

- All staff e-mail messages sent from the Centum shall include an e-mail disclaimer, as follows:

  "Everything in this e-mail and any attachments relating to the official business of CENTUM is proprietary to the company. It is confidential, legally privileged and protected by law. CENTUM does not own and endorse any other content. Any views or opinions presented herein are solely those of the author unless clearly stated as being that of the company.

  The person addressed in the e-mail is the sole authorized recipient. If you receive this message in error, please immediately delete it and all copies of it from your system and notify the sender. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited."

2.11 REVIEW

- It is the responsibility of ICT Manager to regularly review the content of the E-mail Usage Policy.

3.0 INTERNET USE POLICY

3.1 INTRODUCTION

- The Internet is an invaluable tool, providing users with instant access to information and resources at the touch of a button, but it is one with inherent security risks and without guarantees of accuracy, reliability or performance.
- The primary aim in allowing the use of the Internet is to improve the quality of work and productivity, research and to facilitate communication within and Centum

3.2 OBJECTIVE

- The purpose of this policy is to establish acceptable use of the Internet and access to the World Wide Web on machines owned or controlled by the Centum or connected to the Centum networks. The policy sets out the responsibility of individuals using the service in order to maximise the benefits of Internet access whilst minimising the risks.

3.3 ORGANISATIONAL RESPONSIBILITIES

- It is the policy of Centum that all staff will have access to the Internet to help them in their work; therefore all staff members serviced by the Centum computer network have access to the Internet.
- Centum will take all reasonable steps to ensure that staff are aware of company policies, procedures and legal obligations relating to the use of the Internet. This will be done through training and other relevant forms of communication.

3.4 PERSONAL RESPONSIBILITIES

- Access to the Internet is provided primarily for work-related purposes, including communication, research, professional development and training.
- In addition to responsibilities for appropriate use of the internet in the workplace, staff are required to ensure that any information they publish on the internet does not damage the reputation of the Company or breach the confidentiality of individual members of staff and/or partners.

3.4.1 INAPPROPRIATE USE

- No member of staff is permitted to access; display or download from Internet sites that hold offensive material, to do so is considered a serious breach of security and may result in

disciplinary actions. Examples of what is considered offensive material includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political beliefs and disability. This list is not exhaustive. Other than instances that demand criminal prosecution, Centum shall remain the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet.

- Copyrighted material must only be used in accordance with the laws that protect copyright.
- Use of the Internet facility for commercial activities other than in the conduct of the Centum's business is prohibited.
- Intentionally introducing files that cause computer problems is prohibited

3.4.2 CHAT/NEWS GROUPS AND BULLETIN BOARDS

- If you use your corporate identity or your Centum email address to join a chat group, news group or post messages on a bulletin board you are expected to conduct yourself in an honest and professional manner and inline with Centum's brand guidelines. You are responsible for what you write; you should be courteous and inoffensive.
- Unless you are authorized to do so, you are not permitted to write or present views on behalf of Centum Investment Co. Ltd.

3.4.3 POSTING INFORMATION ON SOCIAL NETWORKING SITES & THE INTERNET

- The term Social Networking is used to cover such internet sites as Facebook, Twitter, Google+, MySpace and Bebo. It also includes blog sites, internet homepages and other user interactive services.
- The following must not be uploaded/posted to social networking websites:
    - Person identifiable information of Centum's patners and business associates.
    - Person identifiable information of another Centum employee in relation to their employment including judgements of their performance and character.

- Photographs of another Centum employee taken in the work situation.
- Defamatory statements about Centum, its staff, business or contractors.
- Any information relating to Centum's Investment Business that is not considered public information.

3.4.4 PERSONAL USE

- Staff members are permitted to use the Internet for non-business use provided that it is in accordance with the requirements of this policy; it is in their own time and is not excessive or detrimental to their job performance.
- It is expected that staff will act responsibly in doing this, being aware of the image they are presenting to visitors to their work area. Personal Internet browsing must not distract staff from their work or prevent other Centum staff from using the Internet for work related purposes.

3.4.5 USER NAMES AND PASSWORDS

- Each user is responsible for maintaining the security of their individual login and password. Staff must not share their user name and password with anyone, they should not write passwords down where they could be found nor should they choose passwords that are easily guessable. Users are responsible for logging out fully or using appropriate controls to prevent access to PCs when left unattended.
- Password policy requires a minimum password length of 8 characters. The password must use of both upper- and lower-case letters, one or more numerical digits and special characters

3.5 MONITORING

- Use of the Internet will be monitored, subject to agreed protocols. This is to ensure that, for example, there is no access to inappropriate sites.

- Centum records all Internet access. This information can be made available to line managers who suspect that a member of staff may be using the Internet excessively or inappropriately.

- Centum ICT uses a software package to block inappropriate content and to automatically prevent access to specific types of website such as pornographic, racist, or sites advertising illegal wares. However, appropriate use of the Internet remains the responsibility of the individual member of staff.

3.6 VIRUSES

- The Internet is a major source of computer viruses and other malware the effects of which can range from a minor irritant to a major disaster and all have costs involved in their eradication.

- Although the IT network has background antivirus defences it is still essential to be vigilant and only download material from reputable websites. Programmes and executable files should never be downloaded from the Internet without the permission of the ICT Manager. In the event that a user suspects a virus (such as virus warnings, sudden slowdown, unexpected shutdowns or any other unusual activity) they must stop using that machine and contact the ICT Manager as soon as possible.

3.7 QUESTIONS AND COMPLIANCE

- If you have any questions or comments about the Internet use policy, please contact the ICT Manager.

- If you do not have any questions the Company presumes that you understand and are aware of the requirements of this policy and will adhere to them.

- Failure to comply with the requirements of this policy will be dealt with under the Centum's disciplinary procedures.

4.0 INFORMATION SECURITY POLICY

4.1. INTRODUCTION

This top-level information security policy is a key component of Centum overall information security management framework.

Compliance to this policy is expected of all permanent and contractual staff, partners and third party individuals that interact directly to Centum's information systems

4.2. OBJECTIVES, AIM AND SCOPE

4.2.1. OBJECTIVES

- The objectives of Centum Information Security Policy are to preserve:
  - **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
  - **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
  - **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

4.2.2. POLICY AIM

- The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Centum by:
  - Describing the principals of security and explaining how they shall be implemented in the company.
  - Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
  - Creating and maintaining within the company a level of awareness of the need for Information Security as an integral part of the day to day business.

- Protecting information assets under the control of the company.

4.2.3. SCOPE

- This policy applies to all information, information systems, networks, applications and users of Centum or supplied under contract to it.

4.3 RESPONSIBILITIES FOR INFORMATION SECURITY

- Ultimate responsibility for information security rests with the Chief Executive of Centum, but on a day-to-day basis the ICT Manager shall be responsible for managing and implementing the policy and related procedures.
- Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-
    - The information security policies applicable in their work areas
    - Their personal responsibilities for information security
    - How to access advice on information security matters
- All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.
- The Information Security Policy shall be maintained, reviewed and updated by the ICT Manager. This review shall take place annually.
- Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.
- Each member of staff shall be responsible for the operational security of the information systems they use.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.
- Contracts with external contractors that allow access to the company's information systems shall be in operation before access is allowed. These

contracts shall ensure that the staff or sub-contractors of the external company shall comply with all appropriate security policies.

4.4. LEGISLATION

- Centum is obliged to abide by all relevant Kenyan legislations. The requirement to comply with this legislation shall be devolved to staff, who may be held personally accountable for any breaches of information security for which they may be held responsible. Centum shall comply with all ICT related legislations.

4.5 POLICY FRAMEWORK

4.5.1 MANAGEMENT OF SECURITY

- At top management level, responsibility for Information Security shall reside with the CEO.
- The ICT Manager shall be responsible for implementing, monitoring, documenting and communicating security requirements for the company.

4.5.2. INFORMATION SECURITY AWARENESS TRAINING

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

4.5.3. CONTRACTS OF EMPLOYMENT

- Information security expectations of staff shall be included within appropriate job definitions.

4.5.4. SECURITY CONTROL OF ASSETS

- Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

4.5.5. ACCESS CONTROLS

- Only authorized personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data. These areas include the Filing Room and the Server Room.

4.5.6. USER ACCESS CONTROLS

- Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

4.7. COMPUTER ACCESS CONTROL

- Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

4.8. APPLICATION ACCESS CONTROL

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need. Authorisation to use an application shall depend on the availability of a licence from the supplier.

4.9. EQUIPMENT SECURITY

- In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Laptops will be installed with Encryption software and each staff assigned a laptop will be expected to encrypt sensitive information contained in those laptops.

4.10. COMPUTER AND NETWORK PROCEDURES

- Management of computers and networks shall be controlled through standard documented procedures that have been designed and approved.

4.11. INFORMATION RISK ASSESSMENT

- The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

- Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of Centum's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

4.12. INFORMATION SECURITY EVENTS AND WEAKNESSES

- All information security events and suspected weaknesses are to be reported to the ICT Manager. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

4.13. CLASSIFICATION OF SENSITIVE INFORMATION.

- (See Data Classification & Management Policy)

- A consistent system for the classification of information that are at the discretion of the custodian and there is a low risk of embarrassment or reputational harm to Centum.

- The classification Centum Controlled-shall be used for documents that would otherwise have little on Centum's reputation in the event of disclosure.
- The classification **Centum Confiidential** – shall be used for [to be filled after consultation]
- The classification **Centum Strictly Confidential -** shall be used to mark all other sensitive information such as financial, Employee Records and contractual records. It shall cover information that the disclosure of which is likely to:
    - adversely affect the reputation of the company or its officers or cause substantial distress to individuals;
    - make it more difficult to maintain the operational effectiveness of the company;
    - cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or company's;
    - prejudice the investigation, or facilitate the commission of crime or other illegal activity;
    - breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
    - breach statutory restrictions on disclosure of information
    - disadvantage the company in commercial or Investment negotiations with others or undermine the proper management of the company and its operations.

4.14. PROTECTION FROM MALICIOUS SOFTWARE

- The company shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the company's property without permission from the ICT Manager. Users breaching this requirement may be subject to disciplinary action.

4.15. USER MEDIA

- Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require prior scanning before they may be used on Centum systems. Such media must also be fully virus checked before being used on the company's equipment.

4.16. MONITORING SYSTEM ACCESS AND USE

- An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

- The company shall in place routines to regularly audit compliance with this and other policies. In addition it reserves the right monitor activity where it suspects that there has been a breach of policy. The company shall, where need be keep recording of employees' electronic communications (including telephone communications) for the following reasons:
- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

4.17. ACCREDITATION OF INFORMATION SYSTEMS

- The company shall ensure that all new information systems, applications and networks include a security plan and are approved by the ICT Manager before they commence operation.

4.18. SYSTEM CHANGE CONTROL

- Changes to information systems, applications or networks shall be reviewed and approved by the ICT Manager.

4.19. INTELLECTUAL PROPERTY RIGHTS

- The company shall ensure that all information products are properly licensed and approved by the ICT Manager. Users shall not install software on the company's property without permission from the ICT Manager. Users breaching this requirement may be subject to disciplinary action.

4.20. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

- The company shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

4.21. REPORTING

- The ICT Manager shall keep the Management informed of the information security status of the company by means of regular reports and presentations.

Information Management Policy

5.0 INFORMATION MANAGEMENT POLICY

5.1 PURPOSE

- The purpose of this policy is to support the classification of data enabling the protection of Centum's data, in terms of confidentiality, integrity, and availability. It is also intended to provide guidance on the file naming scheme for the company.

- The policy applies to all members of the Centum staff, including individuals handling data on behalf of the company.

5.2 TERMS

The following terms are used in this document.

- **Availability** - The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis.

- **Confidentiality** - The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include business strategy, investment prospects or staff information, records relating to health, or infrastructure specifications.

- **Data** – Coded representation of quantities, objects and actions. The word "data" is often used interchangeably with the word "information" in common usage.

- **Data custodian** – Individual or group responsible for classifying data and generating guidelines for its lifecycle management. Synonymous with "information custodian."

- **Impact** – A combination of data confidentiality, integrity and availability. Whether a set of data is LOW, MEDIUM, HIGH, or of Very HIGH impact will inform the data classification and whether or not the data set should be considered sensitive data.

- **Information** – Data processed into a form that has meaning and value to the recipient to support an action or decision. "Information" is often used interchangeably with "data" in common usage.

- **Information custodian** – Individual or group responsible for classifying data and generating guidelines for its lifecycle management. Synonymous with "data custodian."

- **Integrity** - The assurance that information is not changed by accident or through a malicious or otherwise criminal act. As Centum's business depends upon the accuracy of data in databases and filing room, Centum must ensure that data is protected from improper change.

5.3 RESPONSIBILITIES

- All Information Owners (Line Managers) are responsible for ensuring that this policy is adopted within their area of responsibility.

- The classification of information will be the responsibility of the Information custodian.

- Individual staff members are responsible for ensuring that sensitive information they produce is appropriately protected and marked with the appropriate classification.

5.4 POLICY REQUIREMENTS FOR INFORMATION ASSETS

- All existing Centum information belongs to one of the classifications below. Unless otherwise classified, information should be treated as **'Centum Internal Use'**.

- All new information assets categorized as confidential or higher should be categorized & labelled for handling according to information handling procedures defined by the Information Owner minimally based on the *Data Classification* described below.

- Controls must be implemented by the Information Owner according to the classification to which the information belongs.

- Information is classified, and may be reclassified, by the Information Owner.

5.5 INFORMATION CLASSIFICATION GUIDE

- This guide provides a framework for classifying and protecting Centum's information resources. It outlines the security objectives in the left column and assesses the potential impact on Centum should certain events occur which jeopardise the information and information systems needed by the company to accomplish its mission, protect its assets, fulfil its legal responsibilities, maintain its day-to-day functions, and protect individuals.

- The three levels of potential impact on Centum or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) are as follows:

    - The *potential impact* is **LOW** if:

- The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on Centum's operations, assets, or on individuals.

- The *potential impact* is **MODERATE** if:
  - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on Centum's operations, assets, or on individuals.

- The potential impact is **HIGH** if
  - The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on Centum's operations, assets, or on individuals.

- **Public information**, i.e. information that can be communicated without restrictions, and is intended for general public use, is not included in the framework below as this data will not cause harm to any individual, group, or to Centum if made public. Examples include: Website Info, Published Statement of Accounts, press releases, event details and advertisements, company profiles.

- In terms of classifying data, if for any one of the data element/combination of elements the potential impact in terms of unauthorised disclosure, unauthorised modification, or loss of data is identified as 'High', then the complete data set should be classified as '**Centum Strictly Confidential**'.

- For example, if in a single data stores copies of invoices classified as 'Centum Internal Use ' occupies the same space as payroll information classified as 'Centum Strictly Confidential', then the classification of Centum Strictly Confidential' applies to the data set.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on Centum's operations, assets, or on individuals.	The unauthorised disclosure of information could be expected to have a serious adverse effect on Centum's operations, assets, or on individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on Centum's operations, assets, or on individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on Centum's operations, assets, or on individuals.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on Centum's operations, assets, or on individuals.	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on Centum's operations, assets, or on individuals.

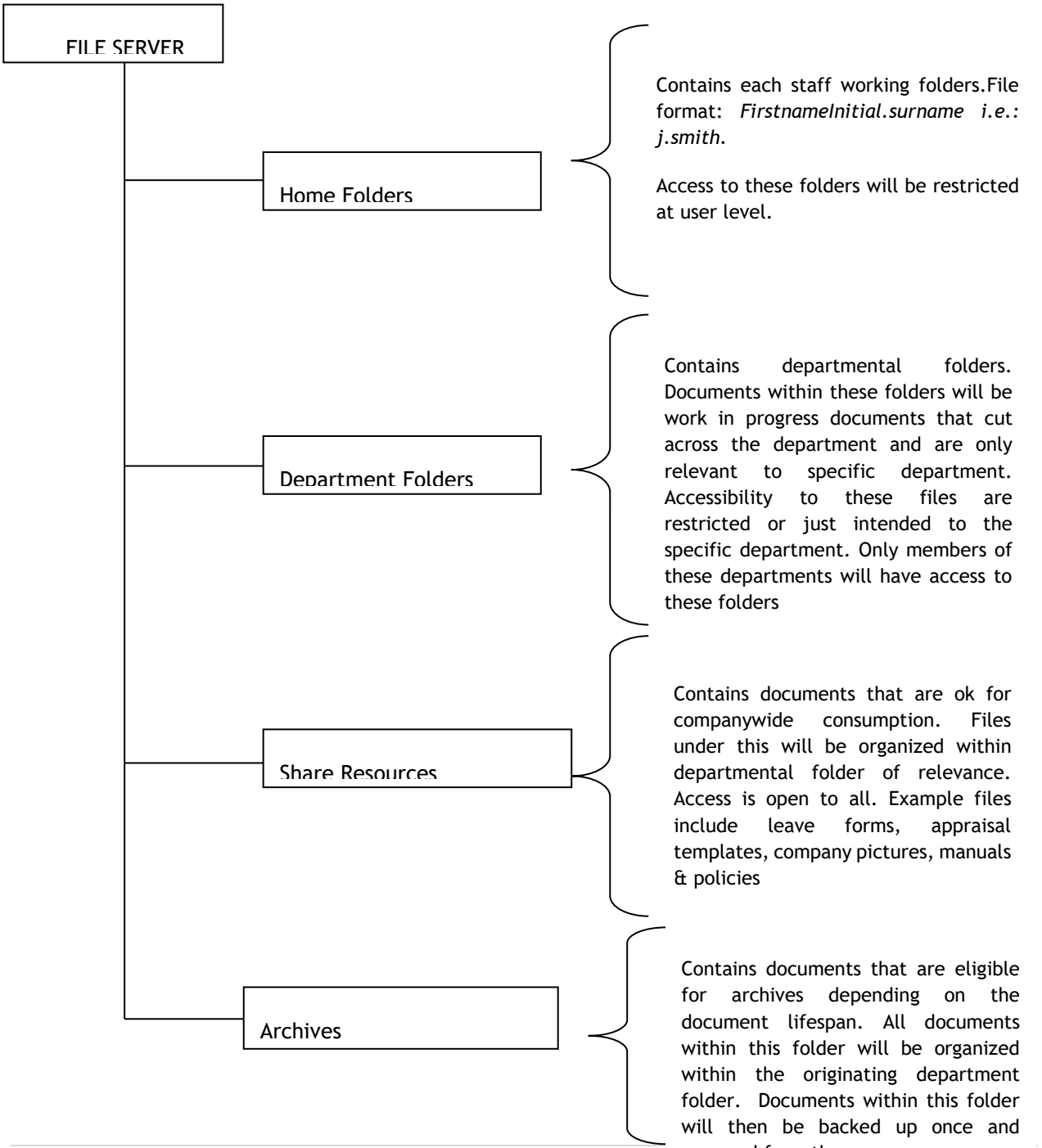
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on Centum's operations, assets, or on individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on Centum's operations, assets, or on individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on Centum's operations, assets, or on individuals.
Data Classification	**Centum Internal Use** With this classification protection of information is at the discretion of the custodian and there is a low risk of embarrassment or reputational harm to Centum. Information not approved for general circulation outside the Company where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to credibility. Security at this level is controlled but normal.	**Centum Confidential** Centum has a legal, regulatory or contractual obligation to protect the information with this classification. Disclosure or loss of availability or integrity could cause harm to the reputation of Centum, or may have short term financial impact on the company.	**Centum Strictly Confidential** Protection of information is required by law or regulatory instrument. The information within this classification is subject to strictly limited distribution within and outside the company. Disclosure would cause exceptional or long term damage to the reputation of Centum, or risk to those whose information is disclosed, or may have serious or long term negative financial impact on the Company.

Examples	Assets Held Review Reports internal memos internal project reports minutes of meetings Financial & Other Models Any other info with equivalent classification from partners	Appraisal Methods bound by NDAs Confidential Information Received from appraisals Unpublished Financial Statements Portfolio deals just materializing Centum Board Packs Investee Board Packs Business plans, Strategy Documents Accounting information Any other info with equivalent classification from partners	Employment Information Passwords & VPN Credentials Contract Information(Centum & 3rd Party) Payroll Information Bank Account Details BOD Minutes Any other info with equivalent classification from partners

5.5 DOCUMENT AND RECORDS MANAGEMENT

Purpose: Standardise documents and records Management within the company so as to enhance document retrieval and identification.

5.6 ELECTRONIC FOLDER ORGANIZATION



5.7 ELECTRONIC FILE NAMING SCHEME

The following rules shall govern folder and file naming

1. Avoid extra long folder names and complex hierarchical structures but use information-rich filenames instead.
2. Put sufficient elements in the structure for easy retrieval and identification but do not overdo it.
3. Use the hyphen (-) to delimit words within an element or capitalize the first letter of each word within an element.
4. Elements should be ordered from general to specific detail of importance as much as possible.
5. Use the hyphen (-
) to delimit words within an element or capitalize the first letter of each word within an element.
6. Elements should be ordered from general to specific detail of importance as mu ch as possible.
7. Personal names within an element should have family name first followed by fir st names or initials.
8. Abbreviate the content of elements whenever possible
9. An element for version control should start with **V** followed by at least 2digits and should be placed as the most last element. To distinguish between working drafts (i.e. minor revisions) use **Vx-01->Vx-99** range and for final draft (i.e. major version release) use V1-**00-> V9-xx**. (where **x =0-9**)
10. Prefix the names of pertinent subfolders to the file name of the files that are being shared via mail

5.8 SCHEME

Files are best named depending on the key element in an event of a search. The different option available considers each of these elements and suggests best possible options;

5.8.1 DATE IS NECESSARY

YYYYMMDD_DPT_FileN_Vn-xx.extension **||**

YYMMDD-DPT_File-Name-Vn-xx.extension

Where: YYYY: Year

MM: Month

DD: Day

DPT: Department

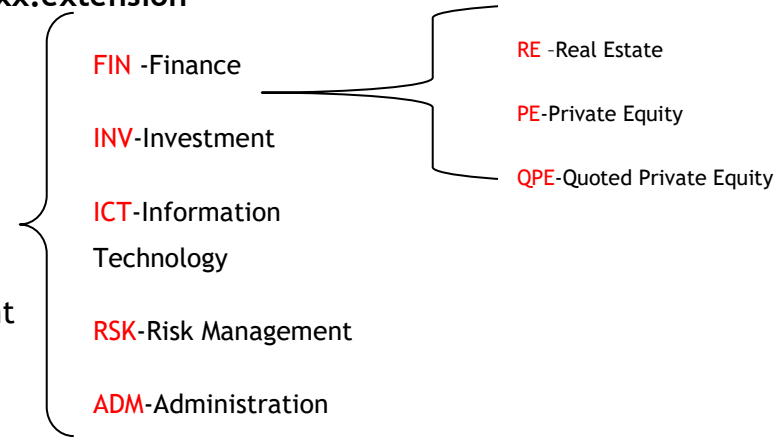
V: Version

n: Number

x: Revision

FileN: File Name

Extension: Document File Extension (e.g. doc,pdf,ppt,jpeg)



5.8.2 RULE OF THUMB:

1. Documents that cut across the Investment Department will have INV as the DPT
2. Documents that are specific to the different sections within Investment Department will have RE, PE or QPE as the DPT instead of INV.

Example;

Naming of a Sale Order memo

20100209_INV_Inv-Policy_V1-01.doc

Naming of a KPLC Model Excel Workbook

20100209_INV_Model-KPLC_V1-09.xls

5.8.3 VARIATION OF DATE

- Financial Year
- Quarter
- Half Year

FY_{YYYY} _Qn_FileN_Vn-xx.extension

FY_{YYYY} : Financial Year

Qn: Quarter Number

Example;

FY2010_Q3_AuditRpt_V3-00.xls

Variation with Company Name

FY2010_KNP_Q3_Bank-Deposit_V0-01.pdf

Variation with Company Name

5.8.4 DATE IS INCONSEQUENTIAL

This will apply to documents that are not time bound. In the event of a search for these documents, the date element or date of creation would not otherwise be important.

Format:

FileN_V-xx.extension

Example;

Perfomance-Appraisal_V1-00.pdf

Leave-form_V2.01.docx

5.8.5 DOCUMENT REFERENCING

To ensure uniformity and tractability of documents and correspondence with third party, all Centum correspondence will have a uniform reference number.

The reference numbers will be in the format;

REF: DEPT/CONTEXT||RECIPIENT/TYPE/YRNo.

Example:

Ref: PE/AON/DIV/10_061….. (Private Equity/AON Minet/Dividend Information/2010_061)

Ref: RA/SRS/BCP/11_001 …… (Risk Analysis/Security Risk Solution/Business Continuity Plan/2011_001)

Where; PE: Department

AON: Company in which we are corresponding to

DIV: Short identifiable subject code

10: The Year

061: Sequence Number of the correspondence

5.9 CONCLUSION

Centum believes that it is important to keep this Data Classification Policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.

Recommendations for changes to this policy should be communicated to the ICT.

ICT Acquisition & Disposal Policy

6.0 ICT ACQUISITION & DISPOSAL POLICY

6.1 INTRODUCTION

This policy defines the process for acquisition of ICT infrastructure and the approved software and hardware standards that are used within Centum Investment.

The aim of the policy is to ensure enterprise wide standardisation enabling ease of ICT governance.

6.2 HARDWARE & SOFTWARE STANDARDS

This section defines hardware and software standard configuration for new PC and Laptop computers. The rationale behind adopting a standard is that it:

- Ensures that the minimum business requirements are met for any computer purchase;
- Will assist departments to identify the appropriate hardware/software configurations when making a request for computing equipment and software to be used for a particular function;
- Will reduce the cost of ownership of equipment purchased by reducing the complexity of the support environment.
- Backup regime in a standardized environment is quicker and easier in the event of a disaster

6.3 HARDWARE

Desktop and Laptops

Going forward, Centum will standardize its Laptop and PC environment to the Lenovo Brand of Machines. The current standard for the period 2009/2013 is Lenovo T4 Series

Minimum Specifications for Laptops are indicated below;

Lenovo ThinkpadT4XX Series

- Intel Core 2 Duo processor P8700 2.53 Ghz,1066Mhz
- 3MB L2 Cache
- 2GB memory

- Intel GM45 Express chipset
- Mobile Intel Graphics Media Accelerator4500MHD
- 250 GB Hard Disk 5400 rpm
- DVD +/- RW
- ExpressCard + 7-in-1 Media Card Reader
- Modem
- 14.1-in WXGA TFT (1280 x 800)
- Bluetooth
- Fingerprint Reader
- WiFi Link 5300 AGN (3 x 3)
- Carrying Case

The warranty period for all new Laptop acquisition will be minimum 3yrs

6.4 SOFTWARE

The following list shows the standard software suites installed on Company Laptops and Desktops that are fully supported by ICT

- Windows XP Pro Service Pack 2/ Windows 7 / Windows 8
- Ms Office 2007 Suite / Ms Office 2013 Suite
- Adobe Acrobat
- Adobe Reader
- Kaspersky Antivirus
- Microsoft Project
- Teamviewer
- WinRAR
- Skype
- FRX
- Microsoft Dynamics GP
- TrueCrypt
- @Risk
- Autodesk 2013

6.5 ADDITIONAL SOFTWARE

A variety of additional software is available for PC and Macintosh. The availability, licensing and support of these packages vary between software packages. If you require other software, licensing information or wish to get advice on the purchase of additional software you should contact the ICT Manager

6.6 ICT ACQUISITION PROCESS

Introduction

The acquisition process will involve the identification and analysis of alternative solutions that are each compared with the established business requirements. The decision making to acquire a typical IT system (Software and Hardware) primarily consists of the following stages:

STAGE 1: Initiation

A need or opportunity is identified and a concept proposal is developed.

STAGE 2: System development concept

Defines the scope, cost benefit analysis, risk management plan and feasibility study.

STAGE 3 Planning

Develops a project management plan and identifies resources need to achieve a solution.

STAGE 4 Requirement analysis

Analyses user needs and develops user requirements. A detailed functional requirement document is created.

STAGE 5: Performing the selection procedure

From the output of the Requirement Analysis Phase, Centum will requests for a proposal from prospective providers, evaluates the proposal, and selects the best available

alternative. Either of the following methods can be used, request for information (RFI), request for bid (RFB), and request for proposal (RFP).

STAGE 6: Proposal evaluation process

The objective of this stage is to define the selection criteria and decide the best match between the product features and functionality with the identified requirements.

1. Examining potential vendors' background. Potential software application providers can be identified from software catalogs, lists provided by hardware vendors, technical and trade journals, or consultants experienced in the other companies, and Web searches. These preliminary evaluation criteria can be used to pre-eliminate the unqualified potential vendors based on the vendor track record, reputation, and some previous feedback.

2. Determining the evaluation criteria. The evaluation criteria will be based on and not limited to: characteristics, of the vendor, functional requirements of the system, technical requirements, total project costs, scalability of the solution, project time frame, quality of documentation provided, and vendor support package.

3. Evaluating providers and their applications. The objective of this evaluation is to determine the gaps between the Centum's needs and the capabilities of the vendors and their application packages.

4. Selecting the provider and its solution. Choosing the vendor and its software depends on the nature of the application. Negotiation can begin with vendors to determine how their packages might be modified to remove any discrepancies with the company's IT needs. Furthermore, feedbacks from the users who will work with the system and the IT staff who will support the system have to be considered. In general, defined list of criteria for selecting a software application package are following:

- Usability and functionality
- Cost-benefit analysis
- Upgrade policy and cost
- Vendor reputation
- System flexibility and scalability
- Manageability
- Quality of documentation

- Hardware and networking resources
- Upgradeability
- Required training
- System security
- Maintenance and operational requirements
- User easiness to learn
- Performance measurement
- Interoperability and data handling
- Ease of integration
- Reliability measurement
- Compatibility with other applications

5. Negotiate a contract. Once the vendor and its package selected, then Centum shall move into the contract negotiation, in which the company shall specify the price of the software/hardware and the type of the support to be provided by the vendor. The contract must describe the detailed specifications, all the included services provided by the vendor, and other detail terms of the system.

6. Establishing a service level agreement (SLA). Centum shall review the vendor supplied SLA that clearly defines:

1. Company and vendor responsibilities,
2. Framework for supply of support services,
3. Company's privilege to have most of the control over the system.

STAGE 7: implementing the selected solution

Upon completion of the contract negotiation, an acceptance plan should be agreed by both the Centum and the vendor so the new application can be ready to be installed or developed.

STAGE 8: Operation & Maintenance

This will include post implementation and in-process reviews. Review of implemented systems will be carried bi-annually to ensure that it conforms to business needs. Upgrades will be conducted as frequent as is necessary to ensure peak performance.

6.7 DISPOSAL OF IT ASSETS

Disposal of ICT assets will be done in accordance to the company's asset disposal policy. All Computers, Servers and handheld devices will be disposed after formatting to factory default.

6.8 APPROVED HARDWARE AND SOFTWARE VENDORS

The ICT Manager shall maintain an updated list of approved software and hardware vendors for each financial period

6.9 REVIEW OF THIS DOCUMENT

This document will be monitored in the light of current hardware and software development.

Laptops and ICT Assets

7.0 LAPTOPS AND ICT ASSETS

7.1 PURPOSE

The purpose of this policy is to outline the acceptable use of laptops by Centum staff. As laptops will be used to access the network, this document must be read in conjunction with the ICT Security Policy.

Inappropriate use of laptops may expose CENTUM to unnecessary risks including information loss, security attacks, compromise of network systems and services, financial and legal issues. Therefore, this policy aims to:

- Guard against theft/loss of the laptop
- Loss/Theft of the information stored on the laptop
- Damage to the equipment
- Promote appropriate use of the laptop computer

7.2 ELIGIBILITY

Providing that resources are available, permanent members of staff will be issued with a laptop at the discretion of Centum management if it is felt necessary for them to carry out their duties.

The appropriate and secure use of laptops will be monitored. Staff will be kept updated with any new developments and receive appropriate training for new or upgraded applications.

Every user who is issued with a laptop will be asked to sign for receipt of the portable device, and to acknowledge that they have read, understood and will comply with this policy.

Due to security threats, users shall require approval of the ICT Manager when they bring their personal laptops to work.

7.3 STAFF RESPONSIBILITY

Staff should take good care of the laptop and take all reasonable precautions to ensure that it is not damaged, lost or stolen. In the event that the device is stolen, staff will be expected to report the theft to the police and obtain an incident number.

Staff members must report the loss of a laptop to their line manager who will subsequently inform ICT Section. Negligence in the care of laptops or failure to report loss or damage at the earliest opportunity may result in disciplinary action being taken against the staff member concerned.

7.4 CARE OF LAPTOPS

A laptop is allocated to a particular member of staff for his or her use and is entrusted to their care. The member of staff should therefore take all reasonable care to secure the laptop and to guard against damage.

7.5 TRANSPORTING LAPTOPS

Laptops should always be within the protective bag supplied with the laptop when carried.

The carrying case can hold objects (such as folders and books), but these must be kept to a minimum to avoid placing too much pressure and weight on the laptop screen.

For short periods of time i.e. moving between meetings, laptops may be put into hibernation (standby mode), thus reducing the start-up time. For longer periods, laptops should be turned off properly before placing it in the carry case.

Care should be taken when placing the laptop in overhead storage compartments e.g. when travelling by bus/air to ensure that the laptop is secure and cannot slide around.

Centum Staff shall only carry laptop’s when travelling with personal cars or cabs but never with public transport vehicles.

7.6 SCREEN CARE

The laptop screen can be damaged if subject to rough treatment. The screen is particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the laptop when it is closed.
- Do not place anything in the carrying case that will press against the cover.
- Do not place anything on the keyboard because forgetting objects (I.e. pens, notebooks) on the keyboard and closing the lid may cause damage to the screen.
- Only clean the screen with soft, dry cloth or anti-static cloth.

7.7 BATTERY USE

In order to prolong battery life, laptops should be powered from the mains supply whenever practical. General information on maintaining battery efficiency is available from ICT Section.

7.8 EXTREME TEMPERATURE, MAGNETIC FIELDS AND X-RAY

Do be aware that extreme temperatures, magnetic fields and exposure to x-ray can cause damage to your laptops

7.9 SECURITY AND STORAGE

Each laptop's serial number will be recorded in the CENTUM inventory of computer equipment database.

7.10 LAPTOPS LEFT IN UNSUPERVISED AREAS

The user must take appropriate security measures to protect the laptop and all its peripherals. When unattended, the laptop must be stored in a secure locked location.

- Laptops must not be left in unsupervised areas. Unsupervised areas include unlocked offices or on top of your desk. Do not leave a meeting or conference room without your laptop. Take it with you.
- Do not leave the laptop in an unlocked vehicle; even if the vehicle is in your driveway or garage.
- Never leave you laptop in plain sight. If you must leave you laptop in a vehicle, the best place is in the boot.
- Car parks are likely areas for thefts from vehicles as they provide wide choice and cover for thieves.

7.11 AIR TRAVEL

When travelling by air, the laptop must be taken into the cabin. Do not check the laptop in as hold baggage.

It is safe to put the laptop through an x-ray security machine, but the laptop must never be put through a metal detector. Security staff may request that the laptop is removed from the carrying case to be inspected more closely.

7.12 ACCEPTABLE USE

Portable devices owned by CENTUM are subject to the same policies and regulations as the laptops.

Files should not be stored on the hard drive of the laptop. Files should be stored on the EDMS folders drive at the earliest opportunity. Local copies of confidential files should be deleted from the hard drive once they have been transferred. No responsibility will be taken if files that solely exist on the hard drive are lost due to mechanical failure or accidental deletion.

7.13 UNACCEPTABLE USE

Laptops must not be used by non CENTUM employees. ICT must be informed if a laptop is loaned to another member of staff within CENTUM.

7.14 MAINTENANCE AND UPDATES

. All laptops go should go through quarterly maintenance schedules. Anti-virus and software's are configured to update automatically when connected to the CENTUM network. Staff must be aware that laptops which have not been connected to the CENTUM network for any period of time may not have most up-to-date protection.

7.15 STAFF ABSENCE

Subject to the details of absence of a member of staff to whom a laptop has been allocated, arrangements may be made for the member of staff covering for the absence to have access to that laptop.

7.16 STAFF LEAVING CENTUM

Staff leaving CENTUM must return their laptop to ICT Section. It is the responsibility of the member of staff leaving CENTUM to ensure that all files have been copied to the server and/or suitable media before the laptop is returned.

Before a laptop is re-issued to a new member of staff, all files on the local hard drive will be deleted and any personal settings or additional hardware or software will be removed.

7.17 INTERNET/E-MAIL AND WIRELESS CONNECTIVITY

Laptops used to connect to the Internet and access e-mail must be used in accordance with CENTUM's Acceptable Use Policies on Internet and E-mail.

Particular attention should be paid to the provisions relating to access to unsuitable material and activities which may compromise network security.

7.18 PERSONAL USE

Limited personal use of laptops is permitted, subject to the restrictions contained in this or any other related policy. Any personal use of laptops is expected to be in the employee's own time and is not to interfere with the person's job responsibilities or the job responsibilities of other employees.

Staff are not permitted to attach personal equipment e.g. printers, cameras, scanners to a laptop without first contacting ICT Section. If permission is granted, drivers, software etc. will be installed by ICT.

Where personal equipment has been installed on a laptop, ICT will not be responsible for any hardware or software support relating to the personal equipment and reserve the right to uninstall if they consider it to be affecting the performance of the laptop.

7.19 TECHNICAL SUPPORT

Laptops in need of repair must be returned to ICT Section. Staff must not attempt to repair any hardware faults under any circumstances. Where available, a replacement may be issued to the staff member whilst the repairs are being carried out. Staff will be asked to collect their laptop when ready and return the "pool" device if issued.

It should be noted that manufacturers' warranties do not normally cover damage caused by misuse or neglect and do not cover replacement batteries.

7.20 INSURANCE

Laptops given to staff on loan are covered by CENTUM insurance policy for use in CENTUM. This policy also covers use of the laptop at home, travelling to and from CENTUM and when the laptop is taken off-site for training or to meetings.

The insurance policy covers accidental and malicious loss and damage.

7.21 MONITORING

Staff should be aware that the use of laptops, including the contents of local drives, is monitored in accordance with this policy.

CENTUM reserves the right to audit correct usage at any time, and the individual may be held liable for illegally held software or material e.g. in breach of copyright legislation.

1.0 INFORMATION MANAGEMENT POLICY

1.1 INTRODUCTION

The Information management policy enables the control of who can access organizational information, what they can do with it, and how long to retain it. It helps enforce compliance with legal and governmental regulations or internal business processes.

The policy seeks to:

- Provide a framework for operating in a uniform, predictable manner and to ensure that information is secure but accessible.
- Provide a basis for safeguarding Centum's Information, Brand image and ensuring conformance to legislative requirements.

1.2 PURPOSE

The purpose of this policy is to provide guidance and direction on the creation and management of information and records and to clarify staff responsibilities. Centum is committed to establishing and maintaining information and records management practices that meet its business needs, accountability requirements and stakeholder expectations.

The benefits of compliance with this policy will be trusted information and records that are well described, stored in known locations and accessible to staff and clients when needed.

This policy is supported by complementary policies and additional guidelines and procedures.

1.3 POLICY STATEMENT

Centum Investments Company Limited and its subsidiaries, information and records are corporate asset, vital both for ongoing operations and also in providing valuable evidence of business decisions, activities and transactions.

There is an expectation that Centum will and is committed to creating and keeping accurate and reliable records to meet this obligation.

In addition, Centum is committed to best-practice standards in principles and practices. It has implemented a fit-for-purpose information and records management practices and systems to ensure the creation, maintenance and protection of reliable records. All

information and records management practices in Centum are to be in accordance with this policy and its supporting procedures.

2.0 SCOPE

This policy applies to Centum staff and contractors, to all aspects of the agency's business and all business information created and received. It covers information and records in all formats including documents, email, voice messages, memoranda, minutes, audio-visual materials and business system data.

The policy also covers all business applications used to create, manage and store information and records including the official records management systems, email, websites, social media applications, databases and business information systems. It also covers both hard and soft copy information. This policy covers information and records created and managed in-house and off-site.

3.0 CREATION AND MAINTENANCE OF INFORMATION AND RECORDS

Business information and records must be created and captured by everyone subject to this policy. Business information and records created should provide a reliable and accurate account of business decisions and actions. Include all necessary information to support business needs including the names, dates and time, and other key information needed to capture the business context.

All business information and records created and received should be captured into an electronic document management system unless they can be disposed of under a normal administrative practice (NAP). Training is offered on when and where to capture records.

4.0 SYSTEMS USED TO MAINTAIN INFORMATION AND RECORDS

Centum primary information and records management system is our electronic document management system (EDMS), known as eInfotree. Where possible, all incoming paper correspondence received by the organization should be converted to digital format and saved into the EDMS. Incoming paper is then filed following the data classification guidelines.

The following business and administrative databases and software applications are endorsed for the capture and storage of specific information and records. These include:

- Finance system: Great Planes
- Real Estate Management: Procore

A full register of endorsed systems used to create or manage information and records can be found at server 192.168.120.4. These endorsed systems appropriately support information and records management processes such as creation and capture, storage, protection of integrity and authenticity, security, access and retention, destruction and transfer.

Corporate records must not be maintained in email folders, shared folders, hard-disks personal drives or external storage media as these lack the necessary functionality to protect business information and records over time. Records created when using social media applications or mobile devices may need to be captured into an endorsed system.

5.0 ACCESS TO INFORMATION AND RECORDS

5.1 SHARING CORPORATE INFORMATION WITHIN CENTUM:

Information and records are a corporate resource to which all staff may have access, except where the nature of the information requires restriction. Access restrictions should not be imposed unnecessarily but should protect:

- Individual staff, shareholder or client privacy
- Sensitive material such as security classified. [read the data classification guidelines]

When handling information, every staff is reminded of their obligations under the …… Code of Conduct, the Crimes Act ……. and …….. Regulations.

5.2 RELEASE OF PUBLICLY AVAILABLE INFORMATION:

Information will be released for public access in accordance to…....., this is not limited to Website Info, Published Statement of Accounts, press releases, event details and advertisements, company profiles.

RETENTION OR DESTRUCTION

Centum records are destroyed when they reach the end of their required retention period set out in Information Classification and Management Policy. Retention periods in records authorities take into account all business, legal regulatory and government

requirements for the records. Centum uses a number of general and agency-specific authorities to determine retention, destruction and transfer actions for its records.

Some records can be destroyed in the normal course of business. These are records of a short-term, facilitative or transitory value that are destroyed as a 'normal administrative practice'. Examples of such records include rough working notes, drafts not needed for future use or copies of records held for reference.

Unauthorized destruction not only risks penalties under the Archives Act but may expose the company to a range of other risks including:

- an inability to comply with regulatory and legislative responsibilities;
- an inability to provide access to information requested by legal discovery action; and
- damage to organizational brand

Staff should not destroy records, other than in accordance with our information management policy and without the approval necessary.

6.0 TRANSFER OF RECORDS

At times certain records may be required to be transferred out of the custody of Centum. This occurs when records of archival value are no longer being actively used. In this instance Centum transfers them to the National Archives. We are still able to access records if a subsequent need arises to consult records in National Archives care. Another instance where records may be transferred is when records are affected by administrative change and are transferred to the inheriting agency.

7.0 ROLES AND RESPONSIBILITIES

ALL EMPLOYEES:

All staff is responsible for the creation and management of information and records as defined by this policy.

Additional responsibilities for certain staff is listed below:

CHIEF EXECUTIVE OFFICER & SENIOR MANAGEMENT:

CEO: The CEO authorizes this policy and promotes compliance with this policy, delegate's responsibility for the operational planning and running of information and

records management to a senior executive officer in the organization and ensures EDMS is adequately resourced.

Senior management: Senior executive officers/managers are responsible for the visible support of, and adherence to, this policy by promoting a culture of compliant information and records management within the organization and contributing to the development of strategic documents such as the information and records management framework and strategy.

INFORMATION & COMMUNICATION TECHNOLOGY DEPARTMENT

Senior ICT Manager: is responsible for overseeing the management of information and records in this organisation consistent with the requirements described in the policy. This includes providing training, advice and general support to staff, creating, developing or acquiring and implementing information and records management products and tools, including systems to assist in the creation of complete and accurate records, developing and implementing strategies to enable sound records management practices, monitoring compliance with information and records management policies and directives and advising senior management of any risks associated with non-compliance.

ICT staff: ICT staff is responsible for maintaining the technology for the business information and records systems, including maintaining appropriate system accessibility, security and back up. ICT staff should ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with this policy. ICT and information and records management staff have an important joint role in ensuring that systems support accountable and effective information and records management across the organization.

MANAGERS AND SUPERVISORS:

Managers and supervisors are responsible for ensuring staff, including contract staff, are aware of, and are supported to follow, the information and records management practices defined in this policy. They should advise the information and records management unit of any barriers to staff complying with this policy. They should also advise the unit of any changes in the business environment which would impact on information and records management requirements, such as new areas of business that need to be covered by a records authority.

8.0 COMMUNICATION AND TRAINING

The policy will be communicated to staff and that training will be provided on aspects of the policy. On conducting training, the policy must be kept up to date; the training should be scheduled regularly and tailored to be meaningful to different workgroups within the organization.

9.0 MONITORING AND REVIEW

This policy will be updated as needed if there are any changes in the business or regulatory environment. It is scheduled for a comprehensive review annually. This review will be initiated by head of information technology unit and conducted by an internal committee of senior management.

Compliance with this policy will be monitored by the information and records management unit. Levels of compliance will be reported at least annually to senior management.