LONGHORN
PUBLISHERS PLC
expanding minds

ICT POLICIES AND PROCEDURES

Joy Kemunto
JANUARY 2021 |

Longhorn Publishers PLC
Funzi Road, Industrial Area

P. O. Box 18033 - 00500 Nairobi, Kenya
Tel: +254 020 6532579/80

Mobile: +254 722 204 608,
+254 708 282 260

www.longhornpublishers.com

Contents

Introduction

The implementation of the reviewed ICT policy establishes a framework for governing information, communication and technology and ensures that Longhorn Publishers PLC adapts to the fast-changing technology landscape.

The manual provides guidelines that ICT will use to administer these policies, with the correct procedure to follow. This framework of policies is intended to be an enabling mechanism for efficient service delivery, information sharing, electronic operations, and reducing information-related risks to acceptable levels.

Access to computers, computing systems and networks owned by Longhorn Publishers PLC enforces certain responsibilities and obligations that are subject to policies and procedures. It is important that these ICT resources are used for the purpose for which they are intended. All users of these resources must comply with specific regulations governing their use, and act responsibly while using shared computing and network resources.

Scope

The areas covered in the ICT Policy Framework.

- Acceptable Use Policy
- Bandwidth Usage Policy
- Backup Policy and Procedures
- OneDrive Cloud Storage
- Password Policy
- User Authentication Policy
- Email Security Policy
- Hardware Management and Use Policy
- Information Security Policy

Audience

This policy framework applies to all users and stakeholders of Longhorn Publishers' ICT systems and to all computer and network systems that are owned and operated by the organization. It is the responsibility of every individual working in Longhorn Publishers PLC to adhere to the regulations provided by the framework.

Acceptable Use Policy

Introduction

Longhorn Publishers PLC allows staff to access the computing and network resources in order to facilitate them in carrying out their duties and the organization expects these resources be used for purposes related to their respective jobs and not be used for unrelated purposes.

These resources include all company owned, licensed, or managed hardware and software, and use of the network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Purpose

The purpose of this policy is to promote the efficient, ethical, and lawful use of the organization's ICT hardware, software, and network resources.

Objectives

The following are the objectives of acceptable use policy:

- Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources provided for use in carrying out day to day activities.
- Ensure that ICT resources are used in an appropriate manner and support the organization's mission and goals.
- Protect the privacy and integrity of data stored on the company's network.

Acceptable Use Policy Statements

1. This policy applies to all users of computing resources owned or managed by Longhorn Publishers PLC.
2. The resources should be used for the purpose for which they are intended.
3. Users must adhere to the confidentiality rules governing the use of passwords and accounts, details of which must not be shared.
4. Users may use only the computers, computer accounts, and computer files for which they have authorization.
5. The organization encourages and promotes the use of email for administrative and professional purposes. Hence, staff must use their respective email in their business communications.
6. The only way to access to the company's network is to have a valid account, and any other way such as plugging own internet to the company's network shall be considered as a violation.
7. All users of the company's network and computing resources are expected to respect the privacy and personal rights of others.
8. The company has the right to block any site or group of sites according to its policies.
9. The company reserves the right to make any amendments in this policy at any time.
10. Users, who discover or find security problems or suspicious activity, must immediately contact ICT department.

Unacceptable Use Policy Statements

1. Users must not use the organization's network in any illegal manner e.g. commercial purposes nor use it to login or browse illegal web sites or content.
2. Users must not disclose their login information and access or copy another user's email, data, programs, or other files.
3. Users must not attempt to violate or compromise the security standards on the company's network, or any other device connected to the network or accessed through the Internet.
4. The organization's network may not be used for the creation, dissemination, storage, and display of obscene or pornographic material, abusive, indecent, obscene, and defamatory or hate literature etc.
5. Users should not create illegal copies or violate copyright protected material to use or save such copies on devices or send them through the network. It also prevents the illegal use such as sending or downloading or publishing any material that violates the laws of the organization.
6. Users are not allowed to indulge into any activity that may adversely affect the ability of others to use the Internet services provided by the company e.g. denial of service attacks, hacking, virus, or consuming gratuitously large amounts of system resources (disk space, CPU time, and network bandwidth) or by deliberately crashing the machine(s).
7. The organization prevents downloading any programs and installing in the company's computers. Any such request should be done through ICT department.
8. ICT is not responsible of the internet content that been browsed by the end user, or problems that might happen to user from browsing untrusted websites.

Bandwidth Usage Policy

Introduction

The bandwidth usage policy is to enhance the internet usage of Longhorn Publishers PLC users by proper management and control of bandwidth. The usage policy sets guidelines important to use bandwidth as a scarce resource to avoid degradation of network performance. It applies to all staff accessing computing and internet resources, whether from computer, laptop, or Bring Your Own Devices (BYOD) used within the premises.

Purpose

The purpose of the bandwidth usage policy is to manage bandwidth use proactively to avoid degradation of network performance. Its usage should be in line with the organization's mission, vision, and strategy.

Objectives

The following are the objectives of the policy:

- To establish awareness and accountability for bandwidth use
- To educate the users of the priority related to internet traffic
- To provide guidelines for responsible use

Bandwidth Usage Policy Statement

1. Bandwidth may be used for any activity supporting publishing, research, and consultancy in such a way that it will not prevent other users from using the same.
2. ICT maintains the right to use monitoring tools that log and analyze bandwidth usage for all users of the network. However, the collected data is to be used exclusively for the purpose of enhancing proper bandwidth usage.
3. ICT maintains the right to block any traffic that is not in line with the organization's mission and vision and that excessively utilizes bandwidth.
4. The department maintains the right to give priority for one type of traffic over the other based on predefined rules.
5. Bandwidth may not be used for monitoring tools that log and tasks that disturb the bandwidth management and optimization system on any machine connected to the network.
6. Users should not involve in activities such as hacking, sexually explicit material, spamming, gambling, terrorism, illegal drugs or violence using the company's resource.

Backup Policy and Procedures

Introduction

The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. Backup and maintenance of data is critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

Purpose

The purpose of the policy is to ensure servers and data continuity and to support the revival and restoration of archived information in the event of a disaster, equipment failure, and/or accidental loss of files.

Objectives

The following are the objectives of the policy:

- To safeguard the information assets of the organization.
- To prevent the loss of data in the case of accidental deletion or corruption of data, system failure or disaster.
- To permit timely restoration of information and business processes should such events occur.
- To manage and secure backup and restoration processes and the media employed within these processes.

Backup Policy and Procedures Policy Statements

Backup Creation

Backups will be created using industry standard data backup software, Veeam, that supports the enterprise level data assurance. Veeam supports the scheduled backups, full and incremental backups as well as centralized

management.

ICT department is responsible for backing up data that is stored in central systems and databases. Data residing on individual workstation hard drives is the responsibility of the user to backup. Users who store data on company's laptop or desktop are responsible for ensuring the data is stored in a way that will ensure it is properly backed up such as OneDrive as shall be discussed in a different policy.

Backup Verification

On a periodic basis, logged information generated from each backup job will be reviewed to identify any incidences and take corrective actions to reduce any risks associated with failed backups. Test restores from backup for each system will be performed.

ICT department will maintain records demonstrating the review of logs and test restores to demonstrate compliance with this policy for auditing purposes.

Storage, Access, and Security

All backup media must be stored in a secure area that is accessible only to designated staff(s). Backup media will be stored in a physically secured place when not in use. During transport or changes of media, media will not be left unattended.

Retirement and Disposal of Media

Prior to retirement and disposal, ICT department will ensure the following:

The media no longer contains active backup images or that any active backup images have been copied to other media.

The media's current or former contents cannot be read or recovered by an unauthorized party.

With all backup media, ICT will ensure the physical destruction of the media prior to disposal.

OneDrive Cloud Storage Policy

Introduction

OneDrive is a convenient way to store files in the "cloud" and protect against hard drive failure, lost or stolen laptops. Keeping your important files in OneDrive means that you have access to them from anywhere provided you have an internet connection.

Purpose

The purpose of this policy is to provide advice and best practices for using cloud storage services to support the processing, sharing and management of organization's data using the existing Microsoft cloud platform.

It is important to keep in mind that ICT department does not have the ability to backup or restore the files that you keep on OneDrive.

OneDrive Cloud Storage Policy Statements

1. OneDrive also allows for easy sharing and collaboration with colleagues. Microsoft provides OneDrive apps for your laptop, desktop, iPads, iPhones, Android devices and Windows Operating System.
2. This service is available to all staff. To use OneDrive, you use the same login and password credentials as you do for Microsoft Outlook.
3. It is important to keep in mind that the organization does not have the ability to backup or restore the files that you keep on OneDrive.
4. ICT department will not be held responsible for any and/or all data loss or corruption.

Password Policy

Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The implementation of the policy will better safeguard the personal and confidential information of all users within the organization. Additionally, this policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

Purpose

This policy establishes a standard for the creation of strong passwords, protection of the passwords, and frequency of change.

Password Policy Objectives

The following are the objectives of the policy:

- Defend against unauthorized access of systems that could result in a compromise of personal or institutional data.
- Ensure that ICT resources are used in an appropriate manner and support the organization's goals.
- Encourage users to understand their own rights and responsibilities for protecting their passwords.
- Protect the privacy and integrity of data stored on the company's network.

Password Policy Statements

Guidelines & Procedures:

- ✓ Passwords must be changed every 60 days.

- ✓ All passwords must meet the definition of a strong password described below.
- ✓ Each successive password must be unique. Re-use of the same password will not be allowed.
- ✓ A user account will be temporarily locked for after 3 consecutive failed logins. Account Lockout Duration: 60 mins.
- ✓ The reset password process will be applied to users who log in for the first time.

Poor, weak passwords have the following characteristics:

- ✓ The password contains less than eight characters.
- ✓ The password is a word found in a dictionary (English or foreign)
- ✓ The password is a common usage word such as:
- ✓ Name of family, pets, friends, co-workers, fantasy characters, etc.
- ✓ Birthdays and other personal information such as address and phone numbers.
- ✓ Word or number patterns like aaabbb, 111222, zyxwvts, 4654321, etc.
- ✓ Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong Password Construction Guidelines:

- ✓ Are at least eight alphanumeric characters long
- ✓ Passwords do not contain user ID
- ✓ Contain no more than two identical characters in a row and are not made up of all numeric or alpha characters
- ✓ Contain at least three of the five following character classes:
- ✓ Lower case characters
- ✓ Upper case characters
- ✓ Numbers
- ✓ Punctuation
- ✓ "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

User Authentication Policy

Introduction

The authentication and access control measures ensure appropriate access to information and processing facilities – including servers, desktops and laptops, applications, and network devices and prevent inappropriate access to such resources.

All users should be authenticated, either by using User IDs and passwords or by stronger authentication such as smartcards or biometric devices (e.g. fingerprint recognition) before they can gain access to any information or systems within the installation.

Purpose

The policy is used to prevent unauthorized users from gaining access to any information or systems within the computer installation.

User Authentication Policy Statements

1. All users should be authenticated, either by using UserIDs and passwords or by stronger authentication such as smartcards or biometric devices before they can gain access to any information or systems within the organization- server room.
2. All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least on a quarterly basis.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least 45 days.

4. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
5. All user level and system level passwords must conform to the password policy guidelines.
6. Two-factor authentication (e.g. smartcards or biometric devices, such as fingerprint recognition) should be applied to users with access to critical business applications or sensitive information and to users with special access privileges or access capabilities from external locations.

Email Security Policy

Introduction

This email security policy describes the rules and guidelines aimed at achieving secure email communication, governing management and make users aware of what is considered as acceptable and unacceptable use of the company's email system.

Purpose

To promote data protection and safeguard the public image of Longhorn Publishers PLC.

Email Security Policy Statements

The following actions are prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to users who did not specifically request such material (email spam). Any form of harassment via email and telephone, whether through language, frequency, or size of messages.
2. Unauthorized use or forging of email header information.
3. Solicitation of email for any other email address other than that of the poster's account with the intent to harass or to collect replies.
4. Creating or forwarding "chain letters", "Quail" or other "pyramid" schemes of any type.
5. Copying unauthorized message or attachment.
6. Replying to spam or clicking links to claim rewards in competitions you have not taken part in.

General Email Etiquettes

Below are tips to ensure email system is used efficiently and professionally.

- ✓ When drafting a new email only include the relevant recipients. This should be guided by the email content and your reporting protocol. Avoid for example using allstaff@longhornpublishers.com when the email is not intended for all staff.
- ✓ When replying to an email note the difference between reply and reply to all. Reply to All is useful only in cases where your feedback is necessary and relevant to all the recipients of the mail. Reply will by default deliver to the sender, but it also allows you to include any other recipient(s).
- ✓ Use BCC and CC appropriately. Both CC and BCC forward a copy of the message to everyone listed. The main difference is that with the BCC the recipients do not get to know each other.
- ✓ Always include a meaningful subject. Lack of a meaningful subject could make the recipient ignore the email or have it categorized as spam/junk.
- ✓ Do not write in capitals and avoid unnecessary bold not unless you are shouting.
- ✓ Proofread your email before sending it to avoid typos.
- ✓ Do not attach unnecessary files, do not forget to attach files if you are supposed to and give your attachments meaningful names.
- ✓ Do not overuse the high priority option and avoid over using urgent and important.
- ✓ Be cautious when using abbreviations and emoticons.
- ✓ Use neutral language.
- ✓ Avoid opening, replying to, or forwarding spam emails.
- ✓ The department Unit may facilitate configuration of office Email on personal devices, but users are responsible for the activities emanating from the created account.

Hardware Management and Use Policy

Introduction

Hardware constitutes the physical computing equipment and resources used by users in their day to day work activities. These policy guidelines intend to facilitate management and use of ICT hardware and equipment.

Purpose

The purpose of this policy is to define, describe and communicate to staff the requirements regarding the acceptable usage of the organization's computer hardware and peripheral devices.

Hardware Management and Use Policy Statements

1. All hardware is the property of Longhorn Publishers PLC. Equipment shall not be removed from the premises without written authorization. Exceptions apply for portable devices where permission has already been granted by relevant offices.
2. Hardware devices shall not be physically moved from one office to another without authorization from relevant ICT staff.
3. Hardware is to be handled carefully and in a professional manner. Physical abuse of the hardware is prohibited.
4. Consuming food or beverages in proximity to any computer hardware is highly discouraged.

Maintenance Guidelines

ICT Department must ensure all equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in good working order. Employees involved with equipment maintenance should:

- ✓ Retain all copies of manufacturer's instructions.
- ✓ Identify recommended service intervals and specifications.
- ✓ Enable a call-out process in event of failure.
- ✓ Ensure only authorized technicians complete any work on the equipment.
- ✓ Record details of all remedial work carried out.
- ✓ Identify any insurance requirements and put the necessary cover.
- ✓ Record details of faults occurrence and remedial actions required. A service history record of equipment shall be maintained so that as equipment becomes older, decisions can be made regarding the appropriate time for it to be replaced.

Information Security Policy

Introduction

An effective information security policy will provide a sound basis for defining and regulating the organization's information assets as well as the information systems that store, process, and transmit company data. The policy will ensure that information is appropriately secured against the adverse effects of breaches in confidentiality, integrity, availability and compliance which would otherwise occur.

Purpose

This policy provides guidelines for the protection and use of information technology assets and resources within the organization to ensure integrity, confidentiality and availability of data and assets.

Information Security Policy Statements

1. For all servers, mainframes and other network assets, the server room area must be secured with adequate ventilation and appropriate access through biometric access to specific staff.
2. All security and safety of all portable equipment such as laptops and tablets will be the responsibility of the employee who has been issued with the device. Users is required to ensure the asset is always kept safely to protect the security of the asset issued to them.
3. In the event of loss or damage, ICT department will assess the security measures undertaken to determine if the employee will be required to reimburse the institution for the loss or damage.

4. All equipment that has internet access and is owned by the organization must have anti-virus software installed. It is the responsibility of ICT to install all anti-virus software and ensure that this software remains up to date on all technology used by the company.
5. All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements.
6. Every employee will be issued with a unique identification code to access the company's technology and will be required to set a password for access.

Policy Review

This policy shall be reviewed every 2 years or when need arises to align it with Longhorn Publishers PLC mandate as well as incorporate dynamics in the Information Communication Technology industry.

The next policy review is scheduled for October 2022.

Sign Off Page

Mr. Michael Mwaura

Chief Finance & Operations Officer

Signature: _____

Date: _____

Mr. Maxwell Wahome

Group Managing Director

Signature: _____

Date: _____