Information Technology Policy

January 2020

Table of Contents

Definitions

Information Systems: All electronic means used to create, store, access, transmit, and use data, information, or communications in the conduct of administrative, instructional, research, or service activities.

Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Authorized User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

Extranet: An intranet that is partially accessible to authorized persons outside of a company or organization.

Account: Any combination of a User ID (sometime referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system. Whereas AFROHUN may have one Information Security Officer, technical management may designate a number of security administrators.

System Administrator: The person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

Trojan Horse: Destructive programs, usually viruses or worms, which are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or removable media, often from another unknowing victim, or may be urged to download a file from a web site or download site.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Spyware: Programs that install and gather information from a computer without permission and reports the information to the creator of the software or to one or more third parties.

Malware: Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse.

Adware: Programs that are downloaded and installed without user's consent or bound with other software to conduct commercial advertisement propaganda through pop-ups or other ways, which often lead to system slowness or exception after installing.

Keyloggers: A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user's screen. Most malicious keyloggers send this data to a third party remotely (such as via email).

Ransomware: A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files, unless a ransom is paid.

Server: A computer program that provides services to other computer programs in the same or other computers. A computer running a server program is frequently referred to as a server, although it may also be running other client (and server) programs.

Security Incident: In information operations, a security incident is an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

E-mail: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

Clear text: Unencrypted data

Full disk encryption: Technique that encrypts an entire hard drive, including operating system and data.

Key: Phrase used to encrypt or decrypt data

Anti-Spoofing: A technique for identifying and dropping units of data, called packets, that have a false source address.

Antivirus: Software used to prevent, detect, and remove malicious software.

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (e-mail): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email spoofing: The forgery of an email header so the message appears to have originated from someone other than the actual source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation to provide sensitive data or perform an action such as processing a wire transfer.

Inbound filters: A type of software-based traffic filter allowing only designated traffic to flow towards a network.

Quarantine: Suspicious email message may be identified by an antivirus filter and isolated from the normal mail inbox.

SPAM: Unsolicited e-mail, usually from Internet sources. It is often referred to as junk e-mail.

Firewall: Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.

Firewall configuration: The system setting affecting the operation of a firewall appliance.

Firewall ruleset: A set of policy statements or instructions used by a firewall to filter network traffic.

Host firewall: A firewall application that addresses a separate and distinct host, such as a personal computer.

Internet Protocol (IP): Primary network protocol used on the Internet.

Network firewall: A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).

Network topology: The layout of connections (links, nodes, etc.) of a computer network.

Simple Mail Transfer Protocol (SMTP): An Internet standard for electronic mail (e- mail) transmission across Internet Protocol (IP) networks.

Virtual private network (VPN): A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with private, secure access to their organization's network.

Beyond reasonable repair: Refers to any and all equipment whose condition requires fixing or refurbishing that is likely to cost as much or more than total replacement.

Chain of Custody (CoC): Refers to the chronological documentation of the custody, transportation, or storage of evidence to show it has not been tampered with prior to destruction.

disposition: Refers to the reselling, reassignment, recycling, donating, or disposal of IT equipment through responsible, ethical, and environmentally sound means.

Non-leased: Refers to any and all IT assets that are the sole property of AFROHUN, that is, equipment not rented, leased, or borrowed from a third-party supplier or partner company.

Obsolete: Refers to any and all equipment that no longer meets requisite functionality.

Surplus: Refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

Security incident: Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include, but are not limited to, unauthorized access, malicious code, network probes, and denial of service attacks.

End points: Any user device connected to a network. End points can include personal computers, personal digital assistants, scanners, etc.

Flow: The traffic that corresponds to a logical connection between two processes in the network.

IP: Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet.

Packet: The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

Member: An individual who has an established, ongoing relationship with AFROHUN. This includes both members and non-members who have co-signed on loans. Examples of non-members include, but are not limited to, the following:

- Non-member joint account holders
- Non-members holding an account in a state-chartered credit union under state law

Service provider: A third party that maintains, processes, or otherwise is permitted access to member information while performing services for AFROHUN.

Member information: Any record maintained by, or on behalf of, AFROHUN that contains information regarding an individual who has an established, ongoing relationship with AFROHUN. This includes records, data, files, or other information in paper, electronic, or other form that are maintained by, or on behalf of, any service provider on behalf of AFROHUN.

Member information system: Any electronic or physical method used to access, collect, store, use, transmit, protect, or dispose of member information.

Virtual Private Network (VPN): A private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Some VPNs allow employees to securely access a corporate intranet while located outside the office.

User Authentication: A method by which the user of a system can be verified as a legitimate user independent of the computer or operating system being used.

Multi-Factor Authentication: A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories:

- Knowledge (something they know)
- Possession (something they have)
- Inherence (something they are)

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

ISDN: There are two flavors of ISDN: BRI and PRI. BRI is used for home/office/remote access. BRI has two "Bearer" channels at 64kb (aggregate 128kb) and 1 D channel for signaling information.

Remote Access: Any access to AFROHUN's corporate network through a non- AFROHUN controlled network, device, or medium.

Split-tunneling: Simultaneous direct access to a non-AFROHUN network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into AFROHUN's corporate network via a Virtual Private network (VPN) tunnel. VPN is a method for accessing a remote network via "tunneling: through the Internet.

IPsec Concentrator: A device in which VPN connections are terminated.

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.

Bring Your Own Device (BYOD): Privately owned wireless and/or portable electronic handheld equipment.

Cloud computing: Is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications,

and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.

Public cloud: Is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

Private Cloud: Is based on the standard cloud computing model but uses a proprietary architecture at an organization's in-house facilities or uses an infrastructure dedicated to a single organization.

Financial information: Is any data for AFROHUN, its employees, members, or other third parties.

Intellectual property: Is any data that is owned by AFROHUN or provided by a third party that would not be distributed to the public.

Other non-public data or information: Are assets deemed the property of AFROHUN.

Other public data or information: Are assets deemed the property of AFROHUN.

Personally Identifiable Information (PII): Is any data that contains personally identifiable information concerning any members, employees, or other third parties.

1. Acceptable Use of Information systems

Overview

Data, electronic file content, information systems, and computer systems at AFROHUN must be managed as valuable organization resources.

Information Technology's (IT) intentions are not to impose restrictions that are contrary to AFROHUN's established culture of openness, trust, and integrity. IT is committed to protecting AFROHUN's authorized users, partners, and the company from illegal or damaging actions by individuals either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP) are the property of AFROHUN.

These systems are to be used for business purposes in serving the interests of AFROHUN and of its partners and members during normal operations.

Effective security is a team effort involving the participation and support of every AFROHUN employee, volunteer, and affiliate who deals with information and/or information systems.

It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at AFROHUN. These rules are in place to protect the authorized user and AFROHUN. Inappropriate use exposes AFROHUN to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct AFROHUN business or interacts with internal networks and business systems, whether owned or leased by AFROHUN, the employee, or a third party.

All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at AFROHUN, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with AFROHUN policies and standards, local laws, and regulations.

Ownership of Electronic Files

All electronic files created, sent, received, or stored on AFROHUN owned, leased, or administered equipment or otherwise under the custody and control of AFROHUN are the property of AFROHUN.

Privacy

Electronic files created, sent, received, or stored on AFROHUN owned, leased, or administered equipment, or otherwise under the custody and control of AFROHUN are not private and may be accessed by AFROHUN IT employees at any time without knowledge of the user, sender, recipient, or owner.

Electronic file content may also be accessed by appropriate personnel in accordance with directives from the regional Manager, Human Resources, or the CEO.

General Use and Ownership

Access requests must be authorized and submitted from departmental supervisors for employees to gain access to computer systems. Authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that the data and files they create on the corporate systems immediately become the property of AFROHUN. Because of the need to protect AFROHUN's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to AFROHUN.

For security and network maintenance purposes, authorized individuals within the AFROHUN IT Department may monitor equipment, systems, and network traffic at any time.

AFROHUN's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

AFROHUN's IT Department reserves the right to remove any non-business related software or files from any system.

Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with this policy and the following policies:

- Account Management
- Anti-Virus
- Owned Mobile Device Acceptable Use and Security
- E-mail
- Internet
- Safeguarding Member Information
- Personal Device Acceptable Use and Security
- Password
- Cloud Computing
- Wireless (Wi-Fi) Connectivity
- Telecommuting

System level and user level passwords must comply with the Password Policy. Authorized users must not share their AFROHUN login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes.

Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Authorized users may access, use, or share AFROHUN proprietary information only to the extent it is authorized and necessary to fulfill the users assigned job duties.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less.

All users must lockdown their PCs, laptops, and workstations by locking (control-alt- delete) when the host will be unattended for any amount of time. Employees must log-off, or restart (but not shut down) their PC after their shift.

AFROHUN proprietary information stored on electronic and computing devices, whether owned or leased by AFROHUN, the employee, or a third party, remains the sole property of AFROHUN. All proprietary information must be protected through legal or technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of AFROHUN proprietary information to their immediate supervisor and/or the IT Department.

All users must report any weaknesses in AFROHUN computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the IT Department.

Users must not divulge dial-up or dial-back modem phone numbers to anyone without prior consent of the AFROHUN IT Department.

Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes.

Unacceptable Use

Users must not intentionally access, create, store, or transmit material which AFROHUN may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, volunteer/director, contractor, consultant, or temporary employee of AFROHUN authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing AFROHUN-owned resources.

System and Network Activities

The following activities are prohibited by users, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by AFROHUN.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AFROHUN or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to IT.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a AFROHUN computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

- Attempting to access any data, electronic content, or programs contained on AFROHUN systems for which they do not have authorization, explicit consent, or implicit need for their job duties.
- Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of AFROHUN IT.
- Installing or using non-standard shareware or freeware software without AFROHUN IT approval.
- Installing, disconnecting, or moving any AFROHUN owned computer equipment and peripheral devices without prior consent of AFROHUN's IT Department.
- Purchasing software or hardware, for AFROHUN use, without prior IT compatibility review.
- Purposely engaging in activity that may;
    - degrade the performance of information systems;
    - deprive an authorized AFROHUN user access to a AFROHUN resource;
    - obtain extra resources beyond those allocated; or
    - circumvent AFROHUN computer security measures.
- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, AFROHUN users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on AFROHUN information systems. The AFROHUN IT Department is the only department authorized to perform these actions.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Access to the Internet at home, from a AFROHUN-owned computer, must adhere to all the same policies that apply to use from within AFROHUN facilities. Authorized users must not allow family members or other non-authorized users to access AFROHUN computer systems.

AFROHUN information systems must not be used for personal benefit.

Incidental Use

As a convenience to the AFROHUN user community, incidental use of information systems is permitted. The following restrictions apply:

- Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.
- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to AFROHUN approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to AFROHUN without prior approval of management.
- Incidental use must not interfere with the normal performance of an employee's
- work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, AFROHUN.
- Storage of personal email messages, voice messages, files, and documents
- within AFROHUN's information systems must be nominal.
- All messages, files, and documents — including personal messages, files, and documents — located on AFROHUN information systems are owned by AFROHUN, may be subject to open records requests, and may be accessed in accordance with this policy.

Review and Acceptance

All AFROHUN staff is responsible for review and acceptance of *Policy 1: Acceptable Use* upon starting work at AFROHUN (see Exhibit A).

New employee onboarding and training shall include this Policy 1 at a minimum, and in addition to all other applicable training and orientation material, and instructions for acceptance shall be provided at that time. Signed acceptance will be received and retained by Information Technology management.

2. Account Management

Overview

Computer accounts are the means used to grant access to AFROHUN's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for AFROHUN usage.

This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at AFROHUN.

Audience

This policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at AFROHUN, including all personnel affiliated with third parties with authorized access to any AFROHUN information system.

Accounts

- All accounts created must have an associated written request by management approval that is appropriate for the AFROHUN system or service.
- All accounts must be uniquely identifiable using the assigned username.
- Shared accounts on AFROHUN information systems are not permitted.
- Reference the Employee Access During Leave of Absence Policy for removing an employee's access while on a leave of absence or vacation.
- All default passwords for accounts must be constructed in accordance with the AFROHUN Password Policy.
- All accounts must have a password expiration that complies with the AFROHUN Password Policy.
- Concurrent connections may be limited for technical or security reasons.
- All accounts must be disabled immediately upon notification of any employee's termination.

Account Management

The following items apply to System Administrators or designated staff:

- Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.
- All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
- Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.
- All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
- Information system accounts are to be reviewed monthly to identify inactive accounts. If an employee or third-party account is found to be inactive for 30 days, the owners

(of the account) and their manager will be notified of pending disablement. If the account continues to remain inactive for 15 days, it will be manually disabled.

- A list of accounts, for the systems they administer, must be provided when requested by authorized AFROHUN management.
- An independent audit review may be performed to ensure the accounts are properly managed.

3. Anti-Virus

Overview

Malware threats must be managed to minimize the amount of downtime realized by AFROHUN's systems and prevent risk to critical systems and member data. This policy is established to:

- Create prudent and acceptable practices regarding anti-virus management
- Define key terms regarding malware and anti-virus protection
- Educate individuals, who utilize AFROHUN system resources, on the responsibilities associated with anti-virus protection

Note: The terms virus and malware, as well as anti-virus and anti-malware, may be used interchangeably.

Purpose

This policy was established to help prevent infection of AFROHUN computers, networks, and technology systems from malware and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

Audience

This policy applies to all computers connecting to the AFROHUN network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC based equipment connecting to the AFROHUN network.

Policy Detail

All computer devices connected to the AFROHUN network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.

The virus protection software must not be disabled or bypassed without IT approval.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server, attached to the AFROHUN network, must utilize AFROHUN IT approved virus protection software and setup to detect and clean viruses that may infect AFROHUN resources.

Each e-mail gateway must utilize AFROHUN IT approved e-mail virus protection software.

All files on computer devices will be scanned periodically for malware.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Service Desk.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the AFROHUN network until the infection has been removed.

Users should:

- Avoid viruses by NEVER opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from the Trash or Recycle Bin.
- Delete spam, chain, or other junk mail without opening or forwarding the item.
- Never download files from unknown or suspicious sources.
- Always scan removable media from an unknown or non-AFROHUN source (such as a CD or USB from a vendor) for viruses before using it.
- Back up critical data on a regular basis and store the data in a safe place. Critical AFROHUN data can be saved to network drives and are backed up on a periodic basis. Contact the AFROHUN IT Department for details.

Because new viruses are discovered every day, users should periodically check the Anti-Virus Policy for updates. The AFROHUN IT Department should be contacted for updated recommendations.

4. Owned Mobile Device Acceptable Use and Security

Overview

Acceptable use of AFROHUN owned mobile devices must be managed to ensure that employees, Board of Directors, and related constituents who use mobile devices to access AFROHUN's resources for business do so in a safe and secure manner.

This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

Purpose

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of AFROHUN's direct control.

This mobile device policy applies to, but is not limed to, any mobile device issued by AFROHUN that contains stored data owned by AFROHUN and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any AFROHUN owned mobile device capable of storing corporate data and connecting to an unmanaged network
- Voice and Video Recorders
- Cameras

This policy addresses a range of threats to, or related to, the use of AFROHUN data:

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware and other threats could be introduced via a mobile device
Compliance	Loss or theft of financial and/or personal and confidential data could expose AFROHUN to the risk of non-compliance with various identity theft and privacy laws

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT.

Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the AFROHUN network.

Audience

This policy applies to all AFROHUN employees, including full and part-time staff, and the Board of Directors who utilize company-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data.

Such access to this confidential data is a privilege, not a right, and forms the basis of the trust AFROHUN has built with its members, suppliers, and other constituents.

Consequently, employment at AFROHUN does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy applies to any corporate owned hardware and related software that could be used to access corporate resources.

The overriding goal of this policy is to protect the integrity of the private and confidential member and business data that resides within AFROHUN's technology infrastructure.

This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources.

A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to AFROHUN's public image.

Therefore, all users employing a AFROHUN owned mobile device, connected to an unmanaged network outside of AFROHUN's direct control, to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Affected Technology

Connectivity of all mobile devices will be centrally managed by AFROHUN's IT Department and will utilize authentication and strong encryption measures. To protect AFROHUN's infrastructure, failure to adhere to these security protocols will result in immediate suspension of all network access privileges.

Responsibilities

It is the responsibility of any employee or Board Member of AFROHUN, who uses a AFROHUN owned mobile device to access corporate resources, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here.

It is imperative that any AFROHUN owned mobile device that is used to conduct AFROHUN business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Access Control

IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to AFROHUN and AFROHUN-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts AFROHUN's systems, data, users, and members at risk.

Prior to initial use on the AFROHUN network or related infrastructure, all mobile devices must be registered with IT. AFROHUN will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored in the IT Document Storage location. Devices that are not on this list may not be connected to the AFROHUN infrastructure. To find out if a preferred device is on this list, an individual should contact the AFROHUN IT Department Service Desk.

Although IT currently allows only listed devices to be connected to the AFROHUN infrastructure, it reserves the right to update this list in the future.

End users who wish to connect such devices to non-corporate network infrastructure to gain access to AFROHUN data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT Department. AFROHUN data is not to be accessed on any hardware that fails to meet AFROHUN's established enterprise IT security standards.

All mobile devices attempting to connect to the AFROHUN network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by AFROHUN's IT Department. Devices that are not corporate issued are not in compliance with IT's security policies and will not be allowed to connect except by provision of the Personal Device Acceptable Use and Security Policy. AFROHUN owned laptop computers may only access the corporate network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) or Internet Protocol Security (IPsec) VPN connection. The SSL or IPsec VPN portal Web address will be provided to users as required. Smart mobile devices such as Smartphones, PDAs, and UMPCs will access the AFROHUN network and data using Mobile VPN software installed on the device by IT.

Security

Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices containing stored data owned by AFROHUN must use an approved method of encryption to protect data. Laptops must employ full drive encryption with an approved software encryption package. No AFROHUN data may exist on a laptop in clear text. All mobile devices must be protected by a strong password. Refer to the AFROHUN password policy for additional information. Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.

All keys used for encryption and decryption must meet complexity requirements described in AFROHUN's Password Policy.

All users of corporate owned mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain AFROHUN data. Users with devices that are not issued by AFROHUN must adhere to the Personal Device Acceptable Use and Security Policy.

To ensure the security of AFROHUN equipment, mobile devices will be transported and stored as specified in the "Mobile Device Transport and Storage" procedure.

Passwords and confidential data should not be stored on unapproved or unauthorized non-AFROHUN devices.

Any corporate owned mobile device that is being used to store AFROHUN data must adhere to the authentication requirements of AFROHUN's IT Department. In addition, all hardware security configurations must be pre- approved by AFROHUN's IT Department before any enterprise data-carrying device can be connected to it.

IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with AFROHUN's overarching security policy.

Employees, Board of Directors, and temporary staff will follow all enterprise- sanctioned data removal procedures to permanently erase company- specific data from such devices once their use is no longer required. For assistance with detailed data wipe procedures for mobile devices, an individual should contact the AFROHUN IT Department Service Desk. This information is found in the IT Document Storage location.

In the event of a lost or stolen mobile device, it is incumbent on the user to report this to IT immediately. AFROHUN shall employ remote wipe technology to remotely disable and delete any data stored on a AFROHUN PDA or cell phone that is reported lost or stolen. If the device is recovered, it can be submitted to IT for re-provisioning.

Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both AFROHUN-owned and personal mobile devices being used within AFROHUN's premises.

IT maintains the process for patching and updating mobile devices. A device's firmware/operating system must be up to date to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of IT for computing platforms (i.e. laptops). /R

IT maintains the process for security audits on mobile devices. Since handheld devices are not completely under the control of AFROHUN, a periodic audit will be performed to ensure the devices are not a potential threat to AFROHUN.

Help and Support

AFROHUN's IT Department will support its sanctioned hardware and software but is not accountable for conflicts or problems caused using unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

Employees, Board of Directors, and temporary staff will not make modifications of any kind to AFROHUN owned and installed hardware or software without the express approval of AFROHUN's IT Department. This includes, but is not limited to, any reconfiguration of the mobile device.

IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the AFROHUN network.

Organizational Protocol

IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. To identify unusual usage patterns or other suspicious activity, the end user agrees to and accepts that his or her access and/or connection to AFROHUN's networks may be monitored to record dates, times, duration of access, etc. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains AFROHUN's highest priority.

The end user agrees to immediately report to his/her manager and AFROHUN's IT Department, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of AFROHUN resources, databases, networks, etc.

AFROHUN will not reimburse employees if they choose to purchase their own mobile devices except in accordance with the Personal Device Acceptable Use and Security Policy. Users will not

be allowed to expense mobile network usage costs.

AFROHUN prohibits the unsafe and unlawful use of mobile devices, including but not limited to, texting, emailing, or any distracting activity while driving, and requires this audience to comply with all state laws in which one is currently operating, regarding same, hands-free requirements, etc.

Before being granted a device and access to AFROHUN resources, a mobile device user must understand and accept the terms and conditions of this policy.

5. Clean Desk

Overview

AFROHUN is committed to protecting the privacy of its employees and members and shall protect the confidentiality of nonpublic information consistent with Ugandan laws

AFROHUN has an obligation to ensure the security and confidentiality of its member records and to protect these records against unauthorized access that could result in any type of loss or inconvenience for its members.

Purpose

The purpose and principle of a "clean desk" policy is to ensure that confidential data is not exposed to individuals who may pass through the area such as members, service personnel, and thieves. It encourages methodical management of one's workspace.

Because of the risk of being compromised, confidential information should always be treated with care.

Policy Detail

To maintain the security and privacy of employees' and members' personal information, AFROHUN employees should observe the "clean desk" rule. All employees should take appropriate actions to prevent unauthorized persons from having access to member information, applications, or data. Employees are also required to make a conscientious check of their surrounding work environment to ensure that there will be no loss of confidentiality to data media or documents.

The clean desk policy applies to:

- Day Planners and Rolodexes that may contain non-public information
- File cabinets, storage cabinets, and briefcases containing sensitive or confidential information
- Any confidential or sensitive data, including reports, lists, or statements. Sensitive data refers to personal information and restricted data. Personal information includes, but is not limited to:
    - An individual's name
    - Driver's license number or identification card number
    - Account number, credit or debit card number, security code, access code,
    - or password that could permit access to an individual's financial account
    - Restricted data is divided into two categories:
    - Personal data, that refers to any combination of information that identifies and describes an individual.

    - Limited data, that refers to electronic information whose unauthorized access, modification, or loss could seriously or adversely affect AFROHUN, its members, and non-members.
- Electronic devices, including cell phones and PDAs
- Keys used to access sensitive information
- Printouts containing sensitive information
- Data on printers, copy machines, and/or fax machines
- Computer workstations and passwords
- Portable media, such as CD's, disks, or flash drives
- Desks or work areas, including white boards and bookshelves

6. E-mail

Overview

E-mail at AFROHUN must be managed as valuable and mission critical resources. Thus, this policy is established to:

- Create prudent and acceptable practices regarding the use of information resources
- Educate individuals who may use information resources with respect to their responsibilities associated with such use
- Establish a schedule for retaining and archiving e-mail

Purpose

The purpose of this policy is to establish rules for the use of AFROHUN email for sending, receiving, or storing of electronic mail.

Audience

This policy applies equally to all individuals granted access privileges to any AFROHUN information resource with the capacity to send, receive, or store electronic mail.

Legal

Individuals involved may be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission
- Knowingly sending or forwarding an attachment that contains a virus

Policy Detail

- Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on AFROHUN's computer systems. AFROHUN can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by AFROHUN, may be subject to open records requests, and may be accessed in accordance with this policy.
- Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to AFROHUN systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.
- Anti-spoofing practices have been initiated for detecting spoofed emails. Employees should be diligent in identifying a spoofed email. If email spoofing has occurred, IT must be immediately notified.
- Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery. Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered. Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm AFROHUN's reputation. The following activities are prohibited by policy:

- Sending e-mail that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability.
- Using e-mail for conducting personal business.
- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.

- Sending e-mail using another person's e-mail account, except when authorized to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Using unauthorized e-mail software.
- Knowingly disabling the automatic scanning of attachments on any AFROHUN personal computer.
- Knowingly circumventing e-mail security measures.
- Sending or forwarding joke e-mails, chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct AFROHUN business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.
- Setting up or responding on behalf of AFROHUN without management approval.
- All confidential or sensitive AFROHUN material transmitted via e-mail, outside AFROHUN's network, must be encrypted. Passwords to decrypt the data should not be sent via email.
- E-mail is not secure. Users must not e-mail passwords, social security numbers, account numbers, pin numbers, dates of birth, mother's maiden name, etc. to parties outside the AFROHUN network without encrypting the data. All user activity on AFROHUN information system assets is subject to logging and review. AFROHUN has software and systems in place to monitor email usage.
- E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of AFROHUN, unless appropriately authorized (explicitly or implicitly) to do so.
- Users must not send, forward, or receive confidential or sensitive AFROHUN information through non-AFROHUN email accounts. Examples of non-AFROHUN e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, Gmail, and e- mail provided by other Internet Service Providers (ISP). Users with non-AFROHUN issued mobile devices must adhere to the Personal Device Acceptable Use and Security Policy for sending, forwarding, receiving, or storing confidential or sensitive AFROHUN information.

Incidental Use

Incidental personal use of sending e-mail is restricted to AFROHUN approved users; it does not extend to family members or other acquaintances. Without prior management approval, incidental use must not result in direct costs to AFROHUN. Incidental use must not interfere with the normal performance of an employee's work duties.
No files or documents may be sent or received that may cause legal liability for or embarrassment to AFROHUN. Storage of personal files and documents within AFROHUN's IT systems should

be nominal.

E-mail Retention

- Messages are retained for 36 months. Emails older than 36 months are subject to automatic purging.
- Deleted and archived emails are subject to automatic purging.
- Appointments, Tasks, and Notes older than the retention period are subject to automatic purging.

E-mail Archive

- Only the owner of a mailbox and the system administrator has access to the archive.
- Messages will be deleted from the online archive 36 months from the original send/receive date.

7. Firewall

Overview

AFROHUN operates network firewalls between the Internet and its private internal network to create a secure operating environment for AFROHUN's computer and network resources. A firewall is just one element of a layered approach to network security.

Purpose

This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to AFROHUN's network and information systems.

The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks
- Block unwanted traffic as determined by the firewall ruleset
- Hide vulnerable internal systems from the Internet
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet
- Log traffic to and from the internal network
- Provide robust authentication
- Provide virtual private network (VPN) connectivity

Policy Detail

All network firewalls, installed and implemented, must conform to the current standards as determined by AFROHUN's IT Department. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this policy.

- Outbound – allows all Internet traffic to authorized groups
- All traffic is authorized by Internet Protocol (IP) address and port The firewalls will provide:
- Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.
- Application proxy – every packet is stopped at the proxy firewall and examined and compared to the rules configured into the firewall.
- Stateful Inspection – a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

The firewalls will protect against:

- IP spoofing attacks – the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
- Denial-of-Service (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets.
- Any network information utility that would reveal information about the AFROHUN domain.

A change control process is required before any firewall rules are modified. Prior to implementation, the Third-Party Vendor and AFROHUN network administrators are required to have the modifications approved by the Head of IT. All related documentation is to be retained for three (3) years.

All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.

Firewall rulesets and configurations require periodic review to ensure they afford the required levels of protection:

AFROHUN must review all network firewall rulesets and configurations during the initial implementation process and periodically thereafter.

Firewall rulesets and configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained, to preserve the integrity of the data, should restoration be required.

Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

Responsibilities

The IT Department is responsible for implementing and maintaining AFROHUN firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and designees as assigned. Password construction for the firewall will be consistent with the strong password creation practices outlined in the AFROHUN Password Policy.

The specific guidance and direction for information systems security is the responsibility of IT. Accordingly, IT will manage the configuration of the AFROHUN firewalls.

If AFROHUN has contracted with a Third Party Vendor to manage the external firewalls. This vendor will be responsible for:

- Retention of the firewall rules
- Patch Management
- Review the firewall logs for:
- System errors
- Blocked web sites
- Attacks
- Sending alerts to the AFROHUN network administrators in the event of attacks or system errors
- Backing up the firewalls

8. Hardware and Electronic Media Disposal

Overview

Hardware and electronic media disposition is necessary at AFROHUN to ensure the proper disposition of all non-leased AFROHUN IT hardware and media capable of storing member information. Improper disposition can lead to potentially devastating fines and lawsuits, as well as possible irreparable brand damage.

Purpose

AFROHUN owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this policy.

Where assets have not reached end of life, it is desirable to take advantage of residual value through reselling, auctioning, donating, or reassignment to a less critical function. This policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner.

AFROHUN's surplus or obsolete IT assets and resources (i.e. laptops, desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and AFROHUN's upgrade guidelines.

All disposition procedures for retired IT assets must adhere to company approved methods.

Policy Detail

Coordinated by AFROHUN's IT Department. The IT Department is responsible for backing up data from IT assets slated for disposition (if applicable) and removing company tags and/or identifying labels. IT is responsible for selecting and approving external agents for hardware sanitization, reselling, recycling, or destruction of the equipment. IT is also responsible for the chain of custody in acquiring credible documentation from contracted third parties that verify adequate disposition and disposal that adhere to legal requirements and environmental regulations.

It is the responsibility of any employee of AFROHUN's IT Department, with the appropriate authority, to ensure that IT assets are disposed of according to the methods in the Hardware and Electronic Media Disposal Procedure. It is imperative that all dispositions are done appropriately, responsibly, and according to IT lifecycle standards, as well as with AFROHUN's resource planning in mind. Hardware asset types and electronic media that require secure disposal include, but are not limited to, the following:

- Computers (desktops and laptops)
- Printers
- Handheld devices
- Servers
- Networking devices (hubs, switches, bridges, and routers)
- Floppy disks
- Backup tapes
- CDs and DVDs
- Zip drives
- Hard drives / Flash memory
- Other portable storage device

10. Security Incident Management

Overview

Security Incident Management at AFROHUN is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify AFROHUN members of the breach.

Purpose

This policy defines the requirement for reporting and responding to incidents related to AFROHUN information systems and operations. Incident response provides AFROHUN with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

This policy applies to all information systems and information system components of AFROHUN. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- Devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities.

In the event a breach of member's information occurs, AFROHUN is required by Uganda law to notify the individual(s) as described in THE COMPUTER MISUSE ACT, 2011.

Policy Detail

Program Organization

- **Computer Emergency Response Plans** - AFROHUN management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, Charter connectivity is interrupted or an isolated malware discovery.
- **Incident Response Plan Contents** - The AFROHUN incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:
    - Specific incident response procedures

- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises
- Identification and coverage for all critical system components
- Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers

- **Incident Response Testing** - at least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.

11. Internet

Overview

Internet access and usage at AFROHUN must be managed as valuable and mission critical resources. This policy is established to:

- Create prudent and acceptable practices regarding the use of the Internet.
- Educate individuals who may use information resources with respect to their responsibilities associated with such use.

Purpose

The purpose of this policy is to establish the rules for the use of AFROHUN Internet for access to the Internet or the Intranet.

Audience

This policy applies equally to all individuals granted access privileges to any AFROHUN information system or resource with the capacity to access the Internet, the Intranet, or both.

Policy Detail

Accessing the Internet

Users are provided access to the Internet to assist them in the performance of their jobs. At any time, at the request of management, Internet access may be revoked. IT may restrict access to certain Internet sites that reduce network performance or are known or found to be compromised with and by malware. AFROHUN will use internet filters to block high-risk content and deny access to any unwanted material or malware in support of the Acceptable Use Policy.

All software used to access the Internet must be part of the AFROHUN standard software suite or approved by IT. Such software must incorporate all vendor provided security patches.

Users accessing the Internet through a computer connected to AFROHUN's network must do so through an approved Internet firewall or other security device. All software used to access the Internet shall be configured to use a proxy or other means of managing or controlling. Bypassing AFROHUN's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using AFROHUN Internet access for: unauthorized access to local and remote computer systems, software piracy, illegal activities, the transmission of threatening, obscene, or harassing materials, or personal solicitations.

Expectation of privacy

Users should have no expectation of privacy in anything they create, store, send, or receive using AFROHUN's Internet access.

Users expressly waive any right of privacy in anything they create, store, send, or receive using AFROHUN's Internet access.

File downloads and virus protection

Users are prohibited from downloading and installing software on their PC without proper authorization from IT. Technical controls may be utilized to limit the download and installation of software.

Downloaded software may be used only in ways that conform to its license and copyrights.

All files, downloaded from the Internet, must be scanned for viruses using AFROHUN approved virus detection software. If a user suspects a file may be infected, he/she must notify IT immediately.

Users are prohibited from using the Internet to deliberately propagate any virus, worm, Trojan Horse, trap-door, or other malicious program.

Monitoring of computer and Internet usage

All user activity on AFROHUN IT assets is subject to logging and review. AFROHUN has the right to monitor and log all aspects of its systems including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

Frivolous use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize

resources to the exclusion of others. These acts include, but are not limited to, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

Personal use, beyond incidental use of the Internet, may be done only on break room PCs and only in compliance with this policy.

Content

AFROHUN utilizes software that makes it possible to identify and block access to Internet sites containing sexually explicit material or other material deemed inappropriate in the workplace. The display, storing, archiving, or editing of such content on any AFROHUN device is prohibited.

Users are prohibited from attempting to access or accessing inappropriate sites from any AFROHUN device. If a user accidentally connects to a site containing such material, the user must disconnect at once and report the incident immediately to IT. AFROHUN Departments may not host their own websites or contract for the hosting of websites by a vendor without the permission of IT.

Content on all AFROHUN hosted web sites must comply with the AFROHUN Acceptable Use of Information Systems and Privacy Policies. No internal data will be made available to hosted Internet websites without approval of IT.

No personal or non-AFROHUN commercial advertising may be made available via hosted AFROHUN web sites.

Transmissions

All sensitive AFROHUN material transmitted over the Internet or external network must be encrypted.

Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

Incidental use

Incidental personal use of Internet access is restricted to AFROHUN approved Users; it does not extend to family members or other acquaintances.

Incidental use must not result in direct costs to AFROHUN.

Incidental use must not interfere with the normal performance of an employee's work duties.

No files or documents may be sent or received that may cause legal liability for, or embarrassment to, AFROHUN.

Storage of personal files and documents within AFROHUN's IT should be nominal.

All files and documents, including personal files and documents, are owned by AFROHUN, may be subject to open records requests, and may be accessed in accordance with this policy.

Reimbursement

An employee, whose position requires him/her to have remote access, will be reimbursed for his/her Internet expenses up to a reasonable amount. An Expense Report will need to be completed and submitted to his/her manager for approval.

12. Log Management

Overview

Most components of the IT infrastructure at AFROHUN are capable of producing logs chronicling their activity over time. These logs often contain very detailed information about the activities of applications and the layers of software and hardware that support those applications.

Logging from critical systems, applications, and services can provide key information and potential indicators of compromise and is critical to have for forensics analysis.

Purpose

Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance. AFROHUN will perform a periodic risk assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilization – how much capacity is used by services
- Security Events – what activity occurred during an incident, and when
- User Activity – what people are doing with services

Policy Detail

Log generation

Depending on the volume of activity and the amount of information in each log entry, logs have the potential of being very large.

Information in logs often cannot be controlled by application, system, or network administrators, so while the listed items are highly desirable, they should not be viewed as absolute requirements.

Application logs

Application logs identify what transactions have been performed, at what time, and for whom. Those logs may also describe the hardware and operating system resources that were used to execute that transaction.

System logs

System logs for operating systems and services, such as web, database, authentication, print, etc., provide detailed information about their activity and are an integral part of system administration.

When related to application logs, they provide an additional layer of detail that is not observable from the application itself. Service logs can also aid in intrusion analysis when an intrusion bypasses the application itself.

Change management logs, that document changes in the IT or business environment, provide context for the automatically generated logs.

Other sources, such as physical access or surveillance logs, can provide context when investigating security incidents.

Client workstations also generate system logs that are of interest, particularly for local authentication, malware detection, and host-based firewalls.

Network logs

Network devices, such as firewalls, intrusion detection/prevention systems, routers, and switches are generally capable of logging information. These logs have value of their own to network administrators, but they also may be used to enhance the information in application and other logs.

Many components of the IT infrastructure, such as routers and network-based firewalls, generate logs. All of the logs have potential value and should be maintained. These logs typically describe flows of information through the network, but not the individual packets contained in that flow.

Other components for the network infrastructure, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers, provide valuable information about network configuration elements, such as IP addresses, that change over time.

Time synchronization

One of the important functions of a log management infrastructure is to relate records from various sources by time. Therefore, it is important that all components of the IT infrastructure have synchronized clocks. AFROHUN uses Network Time Protocol (NTP) for time synchronization.

Use of log information

Logs often contain information that, if misused, could represent an invasion of the privacy of members of AFROHUN. While it is necessary for AFROHUN to perform regular collection and monitoring of these logs, this activity should be done in the least invasive manner.

Baseline behavior

It is essential that a baseline of activity, within the IT infrastructure, be established and tracked as it changes over time. Understanding baseline behavior allows for the detection of anomalous behavior, which could indicate a security incident or a change in normal usage patterns. Procedures will be in place to ensure that this information is reviewed on a regular and timely basis.

Investigation

When an incident occurs, various ad hoc questions will need to be answered. These incidents may be security related, or they may be due to a malfunction, a change in the IT infrastructure, or a change in usage patterns. Whatever the cause of the incident, it will be necessary to retrieve and report log records.

Thresholds shall be established that dictate what level of staff or management response is required for any given log entry or group of entries and detailed in a procedure.

Log record life-cycle management

When logs document or contain valuable information related to activities of AFROHUN's information resources or the people who manage those resources, they are AFROHUN Administrative Records, subject to the requirements of AFROHUN to ensure that they are appropriately managed and preserved and can be retrieved as needed.

Retention

To facilitate investigations, as well as to protect privacy, the retention of log records should be well defined to provide an appropriate balance among the following:

- Confidentiality of specific individuals' activities
- The need to support investigations
- The cost of retaining the records

Care should be taken not to retain log records that are not needed. The cost of long- term retention can be significant and could expose AFROHUN to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.

Log management infrastructure

A log management infrastructure will be established to provide common management of log records. To facilitate the creation of log management infrastructures, system-wide groups will be established to address the following issues:

- Technology solutions that can be used to build log management infrastructures
- Typical retention periods for common examples of logged information

13. Safeguarding Member Information

Overview

This policy addresses the following topics:

- Board Involvement
- Risk Assessment
- Management and Control of Risk
- Member Information Security Controls
    - Vendor Management Review Program
    - Software Inventory
    - Hardware Inventory
    - Critical Systems List
    - Records Management
    - Clean Desk Policy
    - Hardware and Electronic Media Disposal Policy
    - IT Acquisition Policy
    - Incident Response Plan
    - Information Sharing
- Training
- Testing

Purpose

The purpose of this policy is to ensure that AFROHUN complies with existing Ugandan laws, and to ensure that information regarding members is kept secure and confidential.

Policy Detail

It is the policy of AFROHUN to protect the confidentiality, security, and integrity of each member's non-public personal information in accordance with existing state and federal laws. AFROHUN will establish and maintain appropriate standards relating to administrative, technical, and physical safeguards for member records and information.

AFROHUN will maintain physical, electronic, and procedural safeguards, which comply with federal standards, to guard members' non-public personal information.

AFROHUN will not gather, collect, or maintain any information about its members that is not necessary to offer its products and services, to complete member transactions, or for other relevant business purposes.

AFROHUN does not sell or provide any member information to third parties, including list services, telemarketing firms, or outside companies for independent use.

AFROHUN's Information Security Officer is responsible for annually reviewing the program, making any needed adjustments, and coordinating staff training. AFROHUN Management is responsible for ensuring that its departments comply with the requirements of the program.

Information Security

The I.T department is responsible for developing, implementing, and maintaining an effective information security to:

- Ensure the security and confidentiality of member records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to, or use of, such records or information that would result in substantial harm or inconvenience to any member

Management shall report to the Board of Directors, at least annually, on the current status of AFROHUN's Information Security. The Board of Directors will also be notified of any security breaches or violations and the management team's response and recommendations for changes in the Information Security.

Risk Assessment

AFROHUN maintains a risk assessment that identifies potential threats to member information and evaluates the potential impact of the threats.

On an annual basis, the risk assessment is reviewed and updated by the IT department and AFROHUN's Management. AFROHUN's controls are then updated accordingly.

Management and Control of Risk

In order to manage and control the risks that have been identified, AFROHUN will:

- Establish written procedures designed to implement, maintain, and enforce AFROHUN's information security
- Limit access to AFROHUN's member information systems to authorized
- employees only
- Establish controls to prevent employees from providing member information to unauthorized individuals
- Limit access at AFROHUN's physical locations containing member information, such as building, computer facilities, and records storage facilities, to authorized individuals only
- Provide encryption of electronic member information including, but not limited to, information in transit or in storage on networks or systems to which unauthorized individuals may have access.

- Implement dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, member information
- Monitor AFROHUN's systems and procedures to detect actual and attempted attacks on, or intrusions into, the member information systems
- Establish response programs that specify actions to be taken when AFROHUN suspects or detects that unauthorized individual have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies
- Implement measures to protect against destruction, loss, or damage of member information due to environmental hazards, such as fire and water damage or technical failures
- Regularly test, monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of member information, business arrangements, outsourcing arrangements, and internal or external threats to AFROHUN's information security systems

Member information security controls

AFROHUN has established a series of member information security controls to manage the threats identified in the risk assessment. The controls fall into ten categories.

- **Vendor management review program**
  AFROHUN will exercise appropriate due diligence when selecting service providers. When conducting due diligence, management will conduct a documented vendor review process as outlined in the Vendor Due Diligence Procedure.
  All service providers, who may access member information, must complete a Vendor Confidentiality Agreement requiring the provider to maintain the safekeeping and confidentiality of member information in compliance with applicable state and federal laws. Such agreements must be obtained prior to any sharing of member information. Once the agreement has been completed, management will, according to risk, monitor service providers by reviewing audits, summaries of test results, or other evaluations.
- **Software inventory**
  AFROHUN will maintain an inventory of its desktop, server, and infrastructure software. The information from this collection will provide critical information in identifying the software required for rebuilding systems. A template incorporated into the software inventory ensures that the security configuration and configuration standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The software inventory list will be reviewed and updated on a continual basis.
- **Hardware inventory**
  AFROHUN will maintain an inventory of its desktop, server, and infrastructure hardware. The information from this collection will provide critical information in identifying the hardware requirements for rebuilding systems. A template incorporated into the hardware

inventory ensures that AFROHUN standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The hardware inventory list will be reviewed and updated on a continual basis.

- **Critical systems list**
  AFROHUN will maintain a listing of its critical systems. This listing will support critical reliability functions, communications, services, and data. The identification of these systems is crucial for securing member information from vulnerabilities, performing impact analysis, and in preparing for unscheduled events that affect the operations of AFROHUN.
- **Records management**
  The industry wide general principles of records management apply to records in any format. AFROHUN will adhere to policies and procedures for protecting critical records from all outside and unauthorized access. Access to sensitive data will be defined as to who can access which data and under what circumstances. The access will be logged to provide accountability.
  AFROHUN will adhere to the Records Retention Policy for the proper process to dispose of records. Record disposal will be well documented. An inventory will be maintained of the types of records that are disposed of, including certification that the records have been destroyed.
- **Clean desk policy**
  AFROHUN employees will comply with the Clean Desk Policy. This policy was developed to protect sensitive data from being readily available to unauthorized individuals.
- **Hardware and electronic media disposal procedure**
  AFROHUN will take precautions, as outlined in the Hardware and Electronic Media Disposal Policy, to ensure sensitive data cannot be retrieved from retired hardware or electronic media.
- **IT acquisition policy**
  AFROHUN will adhere to policies and procedures for acquisition of computer related items. Computer related purchases will be reviewed by designated IT personnel for compliance with security plans and alignment with operational and strategic plans.
  A review of technology needs will occur during the annual budgeting and work planning processes. Needs will be classified into either current year plans or long-range needs. The acquisition of technology solutions will be assessed to ensure that both current and future needs are met.
- **Incident response plan**
  Incident response is defined as an organized approach to addressing and managing the aftermath of a security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

As required in the Incident Response Plan, AFROHUN will assemble a team to handle any incidents that occur. Necessary actions to prepare AFROHUN and the Incident Response Team will be conducted prior to an incident as required in the Incident Response Plan.

Below is a summary of the steps the IT Department, as well as AFROHUN management, would take:

- The IT Department will immediately investigate the intrusion to:
  - Prevent any further intrusion to the system
  - Determine the extent of the intrusion and any damage caused
  - Take any steps possible to prevent any future such intrusions
- The IT Department will notify Administrative Management and Risk Management of the intrusion. Administrative Management will be responsible for notifying the Board of Directors.
- The IT Department will follow escalation processes and notification procedures as outlined in the Incident Response Plan. Examples include, but are not limited to, notifications to staff, regulatory agencies, law enforcement agencies, or the public.

Training

AFROHUN recognizes that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. AFROHUN will conduct regular IT training through methods such as staff meetings and computer-based tutorial programs. In addition, employees will be trained to recognize, respond to, and where appropriate, report any unauthorized or fraudulent attempts to obtain member information.

All new employees will receive IT Security Training, as part of their orientation training, emphasizing security and IT responsibility. The Training Specialist, or designee, is responsible for training new employees on Information Security.

Testing

AFROHUN will require periodic tests of the key controls, systems, and procedures of the information security program. In accordance with current industry standards, the frequency and nature of such tests shall be determined by the IT Department.

The Head IT will be responsible for reviewing the results of these tests and for making recommendations for improvements where needed.

14. Network Security And VPN Acceptable Use

Overview

This policy is to protect AFROHUN's electronic information from being inadvertently compromised by authorized personnel connecting to the AFROHUN network locally and remotely via VPN**.**

Purpose

The purpose of this policy is to define standards for connecting to AFROHUN's network from any host. These standards are designed to minimize the potential exposure to AFROHUN from damages, which may result from unauthorized use of AFROHUN resources.

Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical AFROHUN internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, SSH, and cable modems, etc.

Audience

This policy applies to all AFROHUN employees, volunteers/directors, contractors, vendors, and agents with a computer or workstation used to connect to the AFROHUN network. This policy applies to remote access connections used to do work on behalf of AFROHUN, including reading or sending email and viewing intranet resources.

Policy Detail

Network Security

Users are permitted to use only those network addresses assigned to them by AFROHUN's IT Department.

All remote access to AFROHUN will either be through a secure VPN connection on a AFROHUN owned device that has up-to-date anti-virus software, or on approved mobile devices (see the AFROHUN Owned Mobile Device Acceptable Use and Security Policy and the Personal Device Acceptable Use and Security Policy).

Remote users may connect to AFROHUN Information Systems using only protocols approved by IT. Users inside the AFROHUN firewall may not be connected to the AFROHUN network at the same time a remote connection is used to an external network.

Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the AFROHUN network without AFROHUN IT approval.

Users must not install network hardware or software that provides network services without AFROHUN IT approval. Non-AFROHUN computer systems that require network connectivity must be approved by AFROHUN IT.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, AFROHUN users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the AFROHUN network infrastructure. Only the IT Department is permitted to perform these actions.

Users are not permitted to alter network hardware in any way.

Remote Access

It is the responsibility of AFROHUN employees, volunteers/directors, contractors, vendors, and agents, with remote access privileges to AFROHUN's corporate network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to AFROHUN.

General access to the Internet, through the AFROHUN network is permitted for employees who have flat-rate services and only for business purposes. AFROHUN employees are responsible to ensure that they:

- Do not violate any AFROHUN policies
- Do not perform illegal activities
- Do not use the access for outside business interests

AFROHUN employees bear responsibility for the consequences should access be misused.

Employees are responsible for reviewing the following topics (listed elsewhere in this policy) for details of protecting information when accessing the corporate network via remote access methods and acceptable use of AFROHUN's network:

- Virtual Private Network (VPN)
- Wireless Communications

Dial-in modem usage is not a supported or acceptable means of connecting to the AFROHUN network.

Requirements

Secure remote access must be strictly controlled. Control will be enforced with Multi- Factor Authentication (MFA).

AFROHUN employees, volunteers/directors, and contractors should never provide their login or email password to anyone, including family members.

AFROHUN employees, volunteers/directors, and contractors with remote access privileges:

- Must ensure that their computer, which is remotely connected to AFROHUN's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Must not use non-AFROHUN email accounts (i.e. Hotmail, Yahoo, AOL), or other external resources to conduct AFROHUN business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for split-tunneling or dual homing is not permitted at any time.

For remote access to AFROHUN hardware, all hardware configurations must be approved by IT.

All hosts that are connected to AFROHUN internal networks, via remote access technologies, must use up-to-date, anti-virus software applicable to that device or platform.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the AFROHUN production network must obtain prior approval from IT.

Virtual Private Network (VPN)

The purpose of this section is to provide guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the AFROHUN corporate network. This applies to implementations of VPN that are directed through an IPsec Concentrator.

This applies to all AFROHUN employees, volunteers/directors, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN's to access the AFROHUN network.

Approved AFROHUN employees, volunteers/directors, and authorized third parties (customers, vendors, etc.) may utilize the benefit of a VPN on a AFROHUN device, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees. Further details may be found in the Remote Access section.

The following guidelines will also apply:

- It is the responsibility of employees or volunteer/directors, with VPN privileges, to ensure that unauthorized users are not allowed access to AFROHUN internal networks.
- VPN use is controlled using a multi-factor authentication paradigm.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
- VPN gateways will be set up and managed by AFROHUN IT.

- All computers connected to AFROHUN internal networks via VPN or any other technology must use up-to-date, anti-virus software applicable to that device or platform.
- VPN users will be automatically disconnected from AFROHUN's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- To ensure protection from viruses, as well as protection of member data, only AFROHUN-owned equipment or non-AFROHUN devices in accordance with the Personal Device Acceptable Use and Security Policy (BYOD) will have VPN and Remote Access.
- Only IT approved VPN clients may be used.
- By using VPN technology, users must understand that their machines are an extension of AFROHUN's network and as such are subject to the same rules and regulations, as well as monitoring for compliance with this policy.

VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a AFROHUN approved VPN configured to drop all unauthenticated and unencrypted traffic and will be provisioned with split-tunneling disabled. As with all AFROHUN computers, Windows or other OS and/or browser Internet proxy settings will be enabled to effectively route Internet access to the device through AFROHUN firewalls and Internet filters.

To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits, support a hardware address that can be registered and tracked (i.e. a MAC address), and support and employ strong user authentication, which checks against an external database such as TACACS+, iDiTJS, or something similar. Any deviation from this practice will be considered on a case-by-case basis.

VPN Approval, Acceptable Use Review and Acceptance

Approval from the head IT or higher authority is required for a user's VPN access account creation. An acceptable use form is attached to the VPN procedure maintained by Information Technology and shall be reviewed and signed by each approved user to acknowledge having read and understood the policy.

Wireless Communications

Access to AFROHUN networks is permitted on wireless systems that have been granted an exclusive waiver by IT for connectivity to AFROHUN's networks.

This section covers any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to AFROHUN's networks do not fall under the review of this policy.

Register Access Points and Cards

All wireless Access Points/Base Stations connected to the corporate network must be registered and approved by IT. If they are installed in corporate PCs, all wireless Network Interface Cards (i.e. PC cards) used in corporate laptop or desktop computers must be registered with IT.

Approved Technology

All wireless LAN access must use AFROHUN approved vendor products and security configurations.

Setting the Service Set Identifier (SSID)

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

15. Personal Device Acceptable Use And Security (BYOD)

Overview

Acceptable use of BYOD at AFROHUN must be managed to ensure that access to AFROHUN's resources for business are performed in a safe and secure manner for participants of the AFROHUN BYOD program. A participant of the BYOD program includes, but is not limited to:

- Employees
- Contractors
- Board of Directors
- Volunteers
- Related constituents who participate in the BYOD program

This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

Purpose

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data using their personal device. This policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the AFROHUN BYOD program which contains stored data owned by AFROHUN, and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices

- Tablets
- Mobile/cellular phones including smartphones
- Any non-AFROHUN owned mobile device capable of storing corporate data and connecting to an unmanaged network

Refer to the Company and Personally Owned Mobile Device Procedure.

This policy addresses a range of threats to, or related to, the use of AFROHUN data:

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware and other threats could be introduced via a mobile device
Compliance	Loss or theft of financial and/or personal and confidential data could expose AFROHUN to the risk of non-compliance with various identity theft and privacy laws

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the AFROHUN network.

Audience

This policy applies to all AFROHUN employees, including full and part-time staff, Board of Directors, volunteers, contractors, freelancers, and other agents who utilize personally-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust AFROHUN has built with its members, suppliers, and other constituents. Consequently,

employment at AFROHUN does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy applies to:

- Any privately owned wireless and/or portable electronic handheld equipment, hereby referred to as BYOD. AFROHUN grants potential participants of the BYOD program the privilege of purchasing and using a device of their choosing at work for their convenience.
- Related software that could be used to access corporate resources.

This policy is intended to protect the security and integrity of AFROHUN's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The Audience, as defined above, must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network. If users do not abide by this policy, AFROHUN reserves the right to revoke this privilege.

The following criteria will be considered initially, and on a continuing basis, to determine if the Audience is eligible to connect a personal smart device to the AFROHUN network.

- Management's written permission and certification of the need and efficacy of BYOD for that Employee
- Sensitivity of data the Audience can access
- Legislation or regulations prohibiting or limiting the use of a personal smart device for AFROHUN business
- Must be listed on the Information Technology Department's list of approved mobile devices
- Audience's adherence to the terms of the Bring Your Own Device Agreement and this policy and other applicable policies
- Technical limitations
- Other eligibility criteria deemed relevant by AFROHUN or IT

Responsibilities of AFROHUN

- IT will centrally manage the BYOD program and devices including, but not limited to, onboarding approved users, monitoring BYOD connections, and terminating BYOD connections to company resources upon the users leave of employment or service to AFROHUN.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable.

- IT reserves the right to refuse, by non-physical means, the ability to connect mobile devices to AFROHUN and AFROHUN-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts AFROHUN's systems, data, users, and members at risk.
- IT will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to the AFROHUN infrastructure. To find out if a preferred device is on this list, an individual should contact the AFROHUN IT department Service Desk. Although IT currently allows only listed devices to be connected to the AFROHUN infrastructure, IT reserves the right to update this list in the future.
- IT will maintain enterprise IT security standards.
- IT will inspect all mobile devices attempting to connect to the AFROHUN network through an unmanaged network (i.e. the Internet) using technology centrally managed by the IT Department.
- IT will install the Mobile VPN software required on Smart mobile devices, such as Smartphones, to access the AFROHUN network and data.

AFROHUN's IT Department reserves the right to:

- Install anti-virus software on any BYOD participating device
- Restrict applications
- Limit use of network resources
- Wipe data on lost/damaged devices or upon termination from the BYOD program or AFROHUN employment
- Properly perform job provisioning and configuration of BYOD participating equipment before connecting to the network
- Through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the AFROHUN network

Responsibilities of BYOD Participants Security and Damages

- All potential participants will be granted access to the AFROHUN network on the condition that they read, sign, respect, and adhere to the AFROHUN policies concerning the use of these devices and services.
- Prior to initial use on the AFROHUN network or related infrastructure, all personally owned mobile devices must be registered with IT.
- Participants of the BYOD program and related software for network and data access will, without exception:

- Use secure data management procedures. All BYOD equipment, containing stored data owned by AFROHUN, must use an approved method of encryption during transmission to protect data.
- Be expected to adhere to the same security protocols when connected with approved BYOD equipment to protect AFROHUN's infrastructure.

- AFROHUN data is not to be accessed on any hardware that fails to meet AFROHUN's established enterprise IT security standards.
  - Ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied to BYOD use.
  - Utilize a device lock with authentication, such as a fingerprint or strong password, on each participating device. Refer to the AFROHUN password policy for additional information.
  - Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.
  - Passwords and confidential data should not be stored on unapproved or unauthorized non-AFROHUN devices.
  - Exercise reasonable physical security measures. It is the end users responsibility to keep their approved BYOD equipment safe and secure.
  - A device's firmware/operating system must be up-to-date in order to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of the owner.
  - Any non-corporate computers used to synchronize with BYOD equipment will have installed anti-virus and anti-malware software deemed necessary by AFROHUN's IT Department. Anti-virus signature files must be up to date on any additional client machines – such as a home PC – on which this media will be accessed.
  - IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.
  - If A) any BYOD device is lost or stolen, immediately contact AFROHUN IT; and, if B) any BYOD device is scheduled to be upgraded or exchanged, the user must contact IT in advance. IT will disable the BYOD and delete associated company data.
  - BYOD equipment that is used to conduct AFROHUN business will be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's access.
  - Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with AFROHUN's overarching security policy.

- Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.
- The user agrees to and accepts that his or her access and/or connection to AFROHUN's networks may be monitored to record dates, times, duration of access, etc. This is done to identify unusual usage patterns or other suspicious activity, and to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains AFROHUN's highest priority.
- Employees, Board of Directors, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of AFROHUN owned and installed hardware or software without the express approval of AFROHUN's IT Department.
- The end user agrees to immediately report to his/her manager and AFROHUN's IT Department, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of AFROHUN resources, databases, networks, etc.

Third Party Vendors

Third party vendors are expected to secure all devices with up-to-date anti-virus signature files and anti-malware software relevant or applicable to a device or platform. All new connection requests between third parties and AFROHUN require that the third party and AFROHUN representatives agree to and sign the Third Party Agreement. This agreement must be signed by the Vice President of the sponsoring department, as well as a representative from the third party who is legally empowered to sign on behalf of the third party. By signing this agreement, the third party agrees to abide by all referenced policies. The document is to be kept on file. All non-publicly accessible information is the sole property of AFROHUN.

The IT Department can supply a non-AFROHUN Internet connection utilizing a Cellular hotspot if needed.

Help and Support

AFROHUN's IT Department is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

16. Password

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of AFROHUN's entire

corporate network. As such, all AFROHUN employees or volunteers/directors (including contractors and vendors with access to AFROHUN systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

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

Audience

This policy applies to all personnel or volunteers/directors who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any AFROHUN facility, has access to the AFROHUN network, or stores any non-public AFROHUN information.

Policy Detail

User Network Passwords

- Passwords for AFROHUN network access must be implemented according to the following guidelines:
- Passwords must be changed every 90 days
- Passwords must adhere to a minimum length of 10 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~';',<>|\).
- Passwords must not be easily tied back to the account owner such as:
- username, social security number, nickname, relative's names, birth date, etc.
- Passwords must not be dictionary words or acronyms
- Passwords cannot be reused for 1 year

System-Level Passwords

- All system-level passwords must adhere to the following guidelines:
- Passwords must be changed at least every 6 months
- All administrator accounts must have 12 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use

Password Protection

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential AFROHUN information.

- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- AFROHUN passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT
- Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.
- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT
- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with AFROHUN.

Application Development Standards

Application developers must ensure their programs follow security precautions in this policy and industry standards.

17. Patch Management

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of AFROHUN’s entire corporate network. As such, all AFROHUN employees or volunteers/directors (including contractors and vendors with access to AFROHUN systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing AFROHUN at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

Given the number of computer workstations and servers that comprise the AFROHUN network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches when they are made available. Effective security is a team effort involving the participation and support of every AFROHUN employee and the Board of Directors.

This policy is to assist in providing direction, establishing goals, enforcing governance, and to outline compliance.

Audience

This policy applies to all employees, contractors, consultants, temporaries, and the Board of Directors at AFROHUN. This policy applies to all equipment that is owned or leased by AFROHUN, such as, all electronic devices, servers, application software, computers, peripherals, routers, and switches.

Adherence to this policy is mandatory.

Policy Detail

Many computer operating systems, such as MacOS, Microsoft Windows, Linux, and others, include software application programs which may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the AFROHUN network, and all computers connected to it. Almost all operating systems and many software applications have periodic security patches, released by the vendor, that need to be applied.

Patches, which are security related or critical in nature, should be installed as soon as possible.

- In the event that a critical or security related patch cannot be centrally deployed by IT, it must be installed in a timely manner using the best resources available.
- Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of policy.

Responsibility

The Head IT is responsible for providing a secure network environment for AFROHUN. It is AFROHUN's policy to ensure all computer devices (including servers, desktops, printers, etc.)

connected to AFROHUN's network, have the most recent operating system, security, and application patches installed.

Every user, both individually and within the organization, is responsible for ensuring prudent and responsible use of computing and network resources.

IT is responsible for ensuring all known and reasonable defenses are in place to reduce network vulnerabilities, while keeping the network operating.

IT Management and Administrators are responsible for monitoring security mailing lists, reviewing vendor notifications and Web sites, and researching specific public Web sites for the release of new patches. Monitoring will include, but not be limited to:

- Scheduled third party scanning of AFROHUN's network to identify known vulnerabilities
- Identifying and communicating identified vulnerabilities and/or security breaches to AFROHUN's IT
- Monitoring Computer Emergency Readiness Team (CERT), notifications, and Web sites of all vendors that have hardware or software operating on AFROHUN's network

The IT Security and System Administrators are responsible for maintaining accuracy of patching procedures which detail what, where, when, and how to eliminate confusion, establish routine, provide guidance, and enable practices to be auditable.

Documenting the implementation details provides the specifics of the patching process, which includes specific systems or groups of systems and the timeframes associated with patching.

Once alerted to a new patch, IT Administrators will download and review the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule.

18. Physical Access Control

Overview

Physical access controls define who is allowed physical access to AFROHUN facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems. Without physical access controls, the potential exits that information systems could be illegitimately, physically accessed and the security of the information they house could be compromised.

Purpose

This policy applies to all facilities of AFROHUN, within which information systems or information system components are housed. Specifically, it includes:

- Server rooms or other facilities for which the primary purpose is the housing of IT infrastructure
- Data rooms or other facilities, within shared purpose facilities, for which one of the primary purposes is the housing of IT infrastructure
- Switch and wiring closets or other facilities, for which the primary purpose is not the housing of IT infrastructure

Policy Detail

Access to facilities, information systems, and information system display mechanisms will be limited to authorized personnel only. Authorization will be demonstrated with authorization credentials (badges, identity cards, etc.) that have been issued by AFROHUN.

Access to facilities will be controlled at defined access points with the use of card readers and locked doors. Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorized personnel are required to authenticate themselves at these access points. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility, without prior authorization, and all deliveries and removals will be logged.

A list of authorized personnel will be established and maintained so that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall be reviewed and, where necessary, updated on at least an annual basis.

If visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified, and must have their authorization verified before physical access is granted. Once access has been granted, visitors must be escorted, and their activities monitored at all times.

19. Cloud Computing Adoption

Overview

Cloud computing would allow AFROHUN to take advantage of technologies for storing and/or sharing documents and other files, and virtual on-demand computing resources. Cloud computing can be beneficial in reducing cost and providing flexibility and scalability.

Purpose

The purpose of this policy is to ensure that AFROHUN can potentially make appropriate cloud adoption decisions and at the same time does not use, or allow the use of, inappropriate cloud

service practices. Acceptable and unacceptable cloud adoption examples are listed in this policy. All other cloud use cases are approved on a case-by-case basis.

Policy Detail

It is the policy of AFROHUN to protect the confidentiality, security, and integrity of each member's non-public personal information. AFROHUN will take responsibility for its use of cloud computing services to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of AFROHUN.

This policy acknowledges the potential use of diligently vetted cloud services, only with:

- Providers who prove, and can document in writing, that they can provide appropriate levels of protection to AFROHUN data in categories that include, but are not limited to, transport, storage, encryption, backup, recovery, encryption key management, legal and regulatory jurisdiction, audit, or privacy
- Explicit procedures for all handling of AFROHUN information regardless of the storage, sharing or computing resource schemes

Cloud Computing Services

The category of cloud service offered by the provider has a significant impact on the split of responsibilities between the customer and the provider to manage security and associated risks.

- Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. The provider is supplying and responsible for securing basic IT resources such as machines, disks, and networks. The customer is responsible for the operating system and the entire software stack necessary to run applications and is responsible for the customer data placed into the cloud computing environment. This means most of the responsibility for securing the applications and the data falls onto the customer.
- Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. The infrastructure, software, and data are primarily the responsibility of the provider, since the customer has little control over any of these features. These aspects need appropriate handling in the contract and the Service Level Agreement (SLA).
- Platform as a Service (PaaS) is a cloud computing service that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Responsibility is likely shared between the customer and provider.

Privacy Concerns

There are information security and data privacy concerns about use of cloud computing services at AFROHUN. They include:

- AFROHUN may be limited in its protection or control of its data, potentially leading to a loss of security, lessened security, inability to comply with various regulations and data handling protection laws, or loss of privacy of data due to aggregation with data from other cloud consumers.
- AFROHUN's dependency on a third party for critical infrastructure and data handling processes.
- AFROHUN may have limited SLAs for a given provider's services and the third parties that a cloud vendor might contract with.
- AFROHUN is reliant on vendors' services for the security of the computing infrastructure.

Diligence

In evaluating the potential use of a particular cloud platform, AFROHUN will pay particular attention to the foregoing, and other privacy concerns, in addition to its documented vendor due diligence program.

Exit Strategy

Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. AFROHUN must determine how data would be recovered from the vendor.

Examples

The following table outlines the data classifications and proper handling of AFROHUN data.

Data Classification	Public Cloud Computing, Storage or Sharing*	Private Cloud and On-premise Computing or Storage User access restricted by username and password or another authentication
Financial Information	Allowed but Not Advised	Allowed No special requirements, subject to any applicable laws
Intellectual Property	Allowed but Not Advised	Allowed No special requirements, subject to any applicable laws
Other Non-Public Data	Allowed but Not Advised	Allowed No special requirements, subject to any applicable laws
Other Public Data	Allowed	Allowed

		No special requirements, subject to any applicable laws
Personally Identifiable Information (PII)	Not Allowed	Allowed No special requirements, subject to any applicable laws

*See Policy 20 Cloud Computing Adoption Appendix A for approved and non- approved services.

20. Server Security

Overview

The servers at AFROHUN provide a wide variety of services to internal and external users, and also store or process sensitive information for AFROHUN. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

Purpose

The purpose of this policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on AFROHUN's internal network(s) or related technology resources via any means. This can include, but is not limited to, the following:

- Internet servers (FTP servers, Web servers, Mail servers, Proxy servers, etc.)
- Application servers
- Database servers
- File servers
- Print servers
- Third-party appliances that manage network resources

This policy also covers any server device outsourced, co-located, or hosted at external/third-party service providers, if that equipment resides in the AFROHUN.org domain or appears to be owned by AFROHUN.

The overriding goal of this policy is to reduce operating risk. Adherence to the AFROHUN Server Security Policy will:

- Eliminate configuration errors and reduce server outages
- Reduce undocumented server configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working

- Protect AFROHUN data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all server equipment that is owned and/or operated by AFROHUN must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all AFROHUN company-owned, company operated, or company controlled server equipment. Addition of new servers, within AFROHUN facilities, will be managed at the sole discretion of IT. Non-sanctioned server installations, or use of unauthorized equipment that manage networked resources on AFROHUN property, is strictly forbidden.

Policy Detail

Responsibilities

AFROHUN's Head IT has the overall responsibility for the confidentiality, integrity, and availability of AFROHUN data.

Supported Technology

All servers will be centrally managed by AFROHUN's IT Department and will utilize approved server configuration standards. Approved server configuration standards will be established and maintained by AFROHUN's IT Department.

All established standards and guidelines for the AFROHUN IT environment are documented in an IT storage location.

- The following outlines AFROHUN's minimum system requirements for server equipment supporting AFROHUN's systems.
- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the Head IT.
- Access to services must be logged or protected though appropriate access control methods.
- Security patches must be installed on the system as soon as possible through
- AFROHUN's configuration management processes.
- Trust relationships allow users and computers to be authenticated (to have their identity verified) by an authentication authority. Trust relationships should be evaluated for their inherent security risk before implementation.
- Authorized users must always use the standard security principle of "Least Required Access" to perform a function.
- System administration and other privileged access must be performed through a secure connection. Root is a user account that has administrative
- privileges which allow access to any file or folder on the system. Do not use the root account when a non-privileged account will do.

- All AFROHUN servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating servers in environments with uncontrolled access (i.e. offices).

This policy is complementary to any previously implemented policies dealing specifically with security and network access to AFROHUN's network.

It is the responsibility of any employee of AFROHUN who is installing or operating server equipment to protect AFROHUN's technology-based resources (such as AFROHUN data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to AFROHUN's public image. Procedures will be followed to ensure resources are protected.

21. Systems Monitoring and Auditing

Overview

Systems monitoring and auditing, at AFROHUN, must be performed to determine when a failure of the information system security, or a breach of the information systems itself, has occurred, and the details of that breach or failure.

Purpose

System monitoring and auditing is used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real time while system auditing looks for them after the fact.

This policy applies to all information systems and information system components of AFROHUN. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities
- Devices that provide centralized storage capabilities
- Desktops, laptops, and other devices that provide distributed computing capabilities
- Routers, switches, and other devices that provide network capabilities
- Firewall, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities

Policy Detail

Information systems will be configured to record login/logout and all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel if inappropriate, unusual, and/or suspicious activity is noted. Inappropriate, unusual, and/or

suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to the head IT or head operations.

Information systems are to be provided with sufficient primary (on-line) storage to retain 30-days' worth of log data and sufficient secondary (off-line) storage to retain one year's worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite the oldest logs. In the event of other logging system failures, the information system will be configured to notify an administrator.

System logs shall be manually reviewed weekly. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.

System logs are considered confidential information. As such, all access to system logs and other system audit information requires prior authorization and strict authentication. Further, access to logs or other system audit information will be captured in the logs.

22. Vulnerability Assessment

Overview

Vulnerability assessments, at AFROHUN, are necessary to manage the increasing number of threats, risks, and responsibilities. Vulnerabilities are not only internal and external, but there are also additional responsibilities and costs associated with ensuring compliance with laws and rules, while retaining business continuity and safety of AFROHUN and member data.

Purpose

The purpose of this policy is to establish standards for periodic vulnerability assessments. This policy reflects AFROHUN's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

This policy covers all computer and communication devices owned or operated by AFROHUN. This policy also covers any computer and communications device that is present on AFROHUN premises, but which may not be owned or operated by AFROHUN. Denial of Service testing or activities will not be performed.

Policy Detail

The operating system or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower the IT Department to perform periodic security risk assessments for determining the area of vulnerabilities and to initiate appropriate remediation. All employees are expected to cooperate fully with any risk assessment.

Vulnerabilities to the operating system or environment for information system resources must be identified and corrected to minimize the risks associated with them.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents and to ensure conformance to AFROHUN's security policies
- Monitor user or system activity where appropriate

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment, the information system resource classification, and the data classification of the data associated with the information system resource.

Retesting will be performed to ensure the vulnerabilities have been corrected. An authenticated scan will be performed by either a Third-Party vendor or using an in-house product.

All data collected and/or used as part of the Vulnerability Assessment Process and related procedures will be formally documented and securely maintained.

IT leadership will make vulnerability scan reports and on-going correction or mitigation progress to senior management for consideration and reporting to the Board of Directors.

23. Website Operation

Overview

The AFROHUN website provides information to members, potential members, and non-members regarding AFROHUN. It is designed to allow members to transact business with AFROHUN and assist non-members with information on how to join AFROHUN. AFROHUN's website may provide links to websites, outside its website, that also serve this purpose.

Purpose

The purpose of this policy is to establish guidelines with respect to communication and updates of AFROHUN's public facing website. Protecting the information on and within the AFROHUN website, with the same safety and confidentiality standards utilized in the transaction of all AFROHUN business, is vital to AFROHUN's success.

Policy Detail

To be successful, the AFROHUN website requires a collaborative, proactive approach by the stakeholders. All stakeholders share the same broad goals and objectives:

- Support the goals and key initiatives of AFROHUN

- Develop content that is member focused, relevant, and valuable, while ensuring the best possible presentation, navigation, interactivity, and accuracy
- Promote a consistent image and identity to enhance information effectiveness
- Periodically assess the effectiveness of web pages

Responsibility

The IT and communications Department are responsible for the website content and ensuring that materials meet legal and policy requirements.

The IT Department is responsible for the security, functionality, and infrastructure of the website. The System Administrators will monitor the AFROHUN website for response time and to resolve any issues encountered.

Links

AFROHUN is not responsible for, and does not endorse, the information on any linked website, unless AFROHUN's website and/or this policy states otherwise. The following criteria will be used to decide whether to place specific links on the AFROHUN website. AFROHUN will place a link on the website if it serves the general purpose of AFROHUN's website and provides a benefit to its members.

AFROHUN's website will provide links to websites for:

- Research Reports, data, tools and educational materials
- Publications and research information on One Health
- Sister organizations, and One health academies
- The AFROHUN website will not provide links to websites for:
    - Illegal or discriminatory activities
    - Political organizations or other organizations advocating a political position on an issue
    - Individual or personal home pages

Security

When a login is required, various forms of multi-factor authentication are implemented to ensure the privacy of member information and security of their transactions.

The AFROHUN website, as well as linked sites, may read some information from the users' computers. The website or linked transactional websites may create and place cookies on the user's computer to ensure the user does not have to answer challenge questions when returning to the site. The multi-factor authentication process will still be required at the next login. This cookie will not contain personally identifying information and will not compromise the user's privacy or security.

Website Changes

Changes to the website will be executed by the AFROHUN IT and Communications Department, another trained and qualified employee, or a specialized firm or individual they may retain, and only with the explicit approval of the CEO or senior executive designated. Website changes require two parties in order to implement.

Website Design

The AFROHUN website maintains a cohesive and professional appearance. While a sophisticated set of services is offered on the website, the goal is to maintain relatively simplistic navigation to ensure ease of use. Security on the website and protection of accurate information is the highest priority in the layout and functionality of the site.

24. Workstation Configuration Security

Overview

The workstations at AFROHUN provide a wide variety of services to process sensitive information for AFROHUN. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

Purpose

The purpose of this policy is to enhance security and quality operating status for workstations utilized at AFROHUN. IT resources are to utilize these guidelines when deploying all new workstation equipment. Workstation users are expected to maintain these guidelines and to work collaboratively with IT resources to maintain the guidelines that have been deployed.

The overriding goal of this policy is to reduce operating risk. Adherence to the AFROHUN Workstation Configuration Security Policy will:

- Eliminate configuration errors and reduce workstation outages
- Reduce undocumented workstation configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect AFROHUN data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all new workstation equipment that is owned and/or operated by AFROHUN must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all AFROHUN company-owned, company operated, or company controlled workstation equipment. Addition of new workstations, within AFROHUN facilities, will be managed at the sole discretion of IT. Non-sanctioned workstation installations, or use of unauthorized equipment that manage networked resources on AFROHUN property, is strictly forbidden.

Policy Detail

Responsibilities

AFROHUN's head of IT has the overall responsibility for the confidentiality, integrity, and availability of AFROHUN data.

Other IT staff members, under the direction of the head of IT, are responsible for following the procedures and policies within IT.

Supported Technology

All workstations will be centrally managed by AFROHUN's IT Department and will utilize approved workstation configuration standards, which will be established and maintained by AFROHUN's IT Department.

All established standards and guidelines for the AFROHUN IT environment are documented in an IT storage location.

The following outlines AFROHUN's minimum system requirements for workstation equipment.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the head of IT.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. AFROHUN has deployed a patch management process; reference the Patch Management Policy.
- All workstations joined to the AFROHUN domain will automatically receive a policy update configuring the workstation to obtain future updates from our desktop management system.
- All systems within AFROHUN are required to utilize anti-virus, malware, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.
- All workstations will utilize the AFROHUN domain so that all general policies, controls, and monitoring features are enabled for each workstation. No system should be managed manually but should be managed through some central tool or model in order to efficiently manage and maintain system security policies and controls.
- Third-party applications need to be updated and maintained. So that software with security updates is not exposed to vulnerabilities for longer than necessary, a quarterly review will be performed.
- Third-party applications, including browsers, shall be updated and maintained in accordance with the AFROHUN patch management program.

- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the IT Department to guarantee the security of the workstations in accordance with the AFROHUN patch management program.
- Internet browsers on workstations will remain up to date. To ensure all browsers are up to date, the IT Department will perform quarterly reviews. If there is a reason the browser cannot be updated, due to conflicts with applications, these exceptions will be recorded.
- By default, all workstations joined to the AFROHUN domain will obtain local security settings through policies.

This policy is complementary to any previously implemented policies dealing specifically with security and network access to AFROHUN's network.

It is the responsibility of each employee of AFROHUN to protect AFROHUN's technology-based resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to AFROHUN's public image. Procedures will be followed to ensure resources are protected.

25. Server Virtualization

Overview

This policy encompasses all new and existing workloads.

Purpose

The purpose of this policy is to establish server virtualization requirements that define the acquisition, use, and management of server virtualization technologies. This policy provides controls that ensure that Enterprise issues are considered, along with business objectives, when making server virtualization related decisions.

Platform Architecture policies, standards, and guidelines will be used to acquire, design, implement, and manage all server virtualization technologies.

Policy Detail

AFROHUN's head of IT has the overall responsibility for ensuring that policies are followed in order to establish contracts and the confidentiality, integrity, and availability of AFROHUN data.

AFROHUN's legacy IT practice was to dedicate one physical server to a single workload. The result of this practice was excessive server underutilization, an ever- expanding data center footprint, and excessive data center power consumption.

Server virtualization software allows the consolidation of new and existing workloads onto high capacity x86 servers. Consolidating workloads onto high capacity x86 servers allows AFROHUN

to reduce the x86 server inventory, which in turn decreases the data center footprint and data center power consumption.

AFROHUN will migrate all new and existing workloads from physical servers to virtual machines. Hardware will be retired at such time as planned by IT management or required by incompatibility with Operating Systems (OS) and/or workload specific software updates.

Server Virtualization Requirements:

- Support industry-wide open-standards
- Embedded security technology, such as, Trusted Platform Module (TPM) or other technologies
- Single centralized management console
- Support industry standard management tools
- Support industry standard backup and recovery tools
- Interoperate with other platform technologies
- Support industry standard x86 hardware
- Support industry standard storage
- Support unmodified guest operating systems
- Functionality to support virtual server management network isolation
- Migrate running guests without interruption
- Add disks to a running guest
- Automatically detect a hardware failure and restart guests on another physical server
- Functionality to configure role-based access for the administrative console
- Support Lightweight Directory Access Protocol (LDAP) for authentication and authorization for administrative console
- Encrypt all intra host and administrative console traffic
- Integrated graphical Central Processing Unit (CPU), memory, disk, and network performance monitoring, alerting, and historical reporting for hosts and guests
- Other industry standard or best in class features as required

26. Wireless (WIFI) Connectivity

Overview

This policy addresses the wireless connection of AFROHUN owned devices in remote locations.

Purpose

The purpose of this policy is to secure and protect the information assets owned by AFROHUN and to establish awareness and safe practices for connecting to free and unsecured Wi-Fi, and that which may be provided by AFROHUN. AFROHUN provides computer devices, networks, and

other electronic information systems to meet missions, goals, and initiatives. AFROHUN grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

Policy Detail

AFROHUN Wi-Fi Network

The AFROHUN Wi-Fi network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it. For employee business use, it is designed to be a supplement to, and not a substitute for, the production wired local area network. For non-employees, it is also provided as a convenience, primarily as a way for members to access AFROHUN internet services. Wi-Fi access points allow for compatible wireless device connectivity.

Microwaves, cordless telephones, neighboring APs, and other Radio Frequency (RF) devices that operate on the same frequencies as Wi-Fi are known sources of Wi-Fi signal interference. Wi-Fi bandwidth is shared by everyone connected to a given Wi-Fi access point (AP). As the number of Wi-Fi connections increase, the bandwidth available to each connection decreases and performance deteriorates. Therefore, the number and placement of APs in a given building is a considered design decision. Due to many variables out of direct AFROHUN control, availability, bandwidth, and access is not guaranteed.

The AFROHUN Wi-Fi network and connection to the Internet shall be:

- Secured with a passphrase and encryption, in accordance with current industry practice
  - Passphrases will be of appropriate complexity and changed at appropriate intervals, balancing security practice with the intended convenient business use of the Wi-Fi
- Physically or logically separate from the AFROHUN production wired local area network (LAN) and its resources
- Provided as a convenience for the use of AFROHUN employees, guests while visiting AFROHUN, the members of AFROHUN, and other visitors with AFROHUN's express permission via provision of an appropriate passphrase
- Optionally provided to members and qualifying visitors, by AFROHUN staff, with the provision of an appropriate passphrase and may be accessed only with the agreement to acceptable use policy statements provided online or in a written or verbal format
- Accessed by employees only in accordance with the Acceptable Use policy and its cross-referenced policies seen in Policy 1 in this document
- Used for access to the AFROHUN production LAN only for business use and with the approved use of a AFROHUN issued virtual private network (VPN) connection

AFROHUN's Wi-Fi service may be changed, the passphrase re-issued or rescinded, the network made unavailable, or otherwise removed without notice for the security or sustainability of AFROHUN business

Public Wi-Fi Usage

When using Wi-Fi on a mobile device in a public establishment, there are precautions that should be followed.

Do:

- As with any Internet-connected device, defend your laptop, tablet, phone, etc. against Internet threats. Make sure your computer or device has the latest antivirus software, turn on the firewall, never perform a download on a public Internet connection, and use strong passwords.
- Look around before selecting a place to sit, consider a seat with your back to a wall and position your device so that someone nearby cannot easily see the screen.
- Assume all Wi-Fi links are suspicious, so choose a connection carefully. A rogue wireless link may have been set up by a hacker. Actively choose the one that is known to be the network you expect and have reason to trust.
- Try to confirm that a given Wi-Fi link is legitimate. Check the security level of the network by choosing the most secure connection, even if you have to pay for access. A password-protected connection (one that is unique for your use) is better than one with a widely shared passphrase and infinitely better than one without a passphrase.
- Consider that one of two similar-appearing SSIDs or connection names may be rogue and could have been setup by a hacker. Inquire of the manager of the establishment for information about their official Wi-Fi access point.
- Avoid free Wi-Fi with no encryption. Even if your website or other activity is using https (with a lock symbol in your browser) or other secure protocols, you are at much greater risk of snooping, eavesdropping, and hacking when on an open Wi- Fi connection
- Seek out Wi-Fi connections that use current industry accepted encryption methods and that generally will require the obtaining of a passphrase from the establishment.
- Consider using your cell phone data plan for sensitive activities rather than untrusted Wi-Fi, or your own mobile hotspot if you have one or have been provided with one.
- If you must use an open Wi-Fi, do not engage in high-risk transactions or highly-confidential communication without first connecting to a virtual private network (VPN).
- If sensitive information absolutely must be entered while using a public network, limit your activity and make sure that, at a minimum, your web browser connection is encrypted with the locked padlock icon visible in the corner of the browser window, and make sure the web address begins with https://. If possible, save your financial transactions for when you are on a trusted and secured connection, at home, for

instance. Passwords, credit card numbers, online banking logins, and other financial information is less secure on a public network.

- Avoid visiting sites that can make it easier or more tempting for hackers to steal your data (for example, banking, social media, and any site where your credit card information is stored).
- If you need to connect to the AFROHUN network and are authorized to do so, choose a trusted and encrypted Wi-Fi AP or use your personal hotspot. In every case, you must use your AFROHUN-provided VPN at all times. The VPN tunnel encrypts your information and communications and besides, hackers are much less likely to be able to penetrate this tunnel and will prefer to seek less secure targets.
- In general, turn off your wireless network on your computer, tablet, or phone when you are not using it to prevent automatic connection to open and possibly dangerous APs. Set your device to not connect automatically to public or unknown and untrusted networks.

Finally,

Do Not:

- Leave your device unattended, not even for a moment. Your device may be subject to loss or theft, and even if it is still where you left it, a thief could have installed a keylogger to capture your keystrokes or other malware to monitor or intercept the device or connection.
- Email or originate other messages of a confidential nature or conduct banking or other sensitive activities, and definitely not when connected to an open, unencrypted Wi-Fi.
- Allow automatic connection to or connection to first Wi-Fi AP your device finds, as it may be a rogue AP set up by a thief. Rather, choose the one that is known to be the network you expect and have reason to trust.

27. Telecommuting

Overview

Telecommuting allows employees to work at home. Telecommuting is a voluntary work alternative that may be appropriate for some employees and some jobs.

Purpose

For the purposes of this policy, reference is made to the defined telecommuting employee who regularly performs their work from an office that is not within a AFROHUN building or suite. Casual telework by employees or remote work by non- employees is not included herein. Focusing on the IT equipment typically provided to a telecommuter, this policy addresses the telecommuting work arrangement and the responsibility for the equipment provided by AFROHUN.

Policy Detail

Telecommuting arrangements are made on a case-by-case basis, focusing first on the business needs of the organization.

The company may provide specific equipment for the employee to perform his/her current duties. This may include computer hardware, computer software, mobile phone, email, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary. In order to purchase, configure, ship, and install the required equipment to the remote location, the IT Department shall be notified in advance of the telecommuting start date.

The use of equipment, software, and data supplies, when provided by AFROHUN for use at the remote work location, is limited to authorized persons and for purposes relating to AFROHUN business. AFROHUN will provide for repairs to or replacement of provided equipment. Damage to equipment owned by AFROHUN, that is outside the employee's control, will be covered by the organization's insurance policy. In the event of such damage, loaner equipment may be provided when available and must be returned upon request.

The IT Department will be responsible for all equipment installation, maintenance, security access, support, and necessary training related to AFROHUN equipment and software at the remote site, even in the event IT chooses to outsource services. All provided, qualified equipment will be tracked in the IT asset program.

The employee shall designate a workspace, within the remote work location, for placement and installation of equipment to be used while teleworking. The employee shall maintain this workspace in a safe condition, free from hazards and other dangers to the employee and equipment. All AFROHUN materials should be kept in the designated work area at home and not made accessible to others. All applicable policies for acceptable use, protection of member information, security, reimbursement of business voice and Internet charges, etc., shall be observed. Personally owned equipment may not be connected to AFROHUN owned equipment.

The employee understands and agrees to the following:

1. The employee is responsible for securing the equipment provided to the employee by the AFROHUN IT Department.
2. No personally owned equipment may be connected to the AFROHUN owned equipment.
3. This equipment is the sole and exclusive property of AFROHUN.
4. With the exception of normal wear and tear, the employee is liable for the condition of the equipment and for any damages caused by any misuse, negligence, and/or unauthorized use of the equipment.
5. The employee will not modify any AFROHUN equipment without written authorization from the IT Department.

6. In the event of equipment failure, the employee will notify the IT Department as soon as possible. AFROHUN may supply temporary equipment in the event of equipment failure.
7. All equipment provided by AFROHUN is provided exclusively for use in providing services to AFROHUN. Only the employee may use the equipment and only for AFROHUN business-related purposes.
8. Within five (5) business days after the employee ceases to telecommute or after termination of employment at AFROHUN, the employee shall return all supplied equipment to the IT Department. If it should become necessary for AFROHUN to resort to legal or other means to recover its equipment, the employee agrees to pay all related costs and attorneys' fees that may be incurred by AFROHUN.

28. Internet of Things IoT

Overview

IoT devices may be business oriented, consumer based, or a hybrid of both. The devices may be company provided or employee owned, such as through a BYOD policy.

Purpose

The purpose of this policy is to establish a defined IoT structure to ensure that data and operations are properly secured. IoT devices continue making inroads in the business world; therefore, it is necessary for AFROHUN to have this structure in place.

Policy Detail

IoT Device Procurement

IoT devices that are to be used for company operations should be purchased and installed by IT personnel.

Employee-owned IoT devices used for business purposes must be used in accordance with Policy 16, Personal Device Acceptable Use and Security (BYOD).

The use of all IoT devices, whether company provided, or employee owned, should be requested via Addendum A, IoT Device Usage Request Form and submitted to the IT department for approval. Only manager level employees and above may request the usage and/or procurement of IoT devices.

The IT department is responsible for identifying compatible platforms, purchasing equipment, and supporting organization provided and authorized IoT devices.

Cybersecurity Risks and Privacy Risk Considerations

It is important for AFROHUN to understand the use of IoT because many IoT devices affect cybersecurity and privacy risks differently than IT devices do. Being aware of the existing IoT usage and possible future usage will assist AFROHUN in understanding how the characteristics of IoT affect managing cybersecurity and privacy risks, especially in terms of risk response.

It is important for AFROHUN to manage cybersecurity and privacy risk for IoT devices versus conventional IT devices, determining how those risk considerations might impact risk management in general, risk response and particularly mitigation, and identifying basic cybersecurity and privacy controls AFROHUN may want to consider, adapt, and potentially include in requirements when acquiring IoT devices. The IoT Risk Management Guide contains insight as to the differences in risk between conventional IT devices and IoT devices. This document resides in the IT document storage area.

Appendix A

Approved Public Cloud Services

This listing is not represented to be exhaustive and is meant to serve as a point-in-time list of approved or disapproved public cloud services as of the revision date in this appendix. Any cloud service not explicitly listed as approved should be assumed to be not approved until documented otherwise.

Services Approved for AFROHUN Use	Services Not Approved for AFROHUN Use
Microsoft365	Personal Cloud Storages
Microsoft OneDrive	
BOX	
ZOOM	
ADOBE	
Microsoft AZURE	
Amazon Web Services	

Digital Ocean	
Google Cloud	

EXHIBIT A

[This exhibit is a copy of the current Acceptable Use of Information Systems receipt.]

Receipt of Acceptable Use of Information Systems

Please sign this form and return it to Information Systems

I have received a copy of the AFROHUN LLC Acceptable Use of Information Systems Policy.

I understand the information in the Acceptable Use of Information Systems policy is a summary only, and it is my responsibility to review and become familiar with all of the material contained in the Comprehensive IT Policy.

I understand the most updated policies and Bylaws will always be located on the intranet for my reference, and it will be my responsibility to review the policies and Bylaws as they are updated.

I further understand the content of the Comprehensive IT Policy supersedes all policies previously issued. I also understand that AFROHUN may supersede, change, eliminate, or add to any policies or practices described in the Comprehensive IT Policy.

My signature below indicates that I have received my personal copy of the Acceptable Use of Information Systems Policy and it will be my responsibility to review the Comprehensive IT policies as they are updated.

User Signature_____

User Name (printed)_____

Date:_____

***Retain one copy of this Receipt for your records and return the other copy to Information Systems.*

EXHIBIT B

AFROHUN Owned Mobile Device Agreement

This AFROHUN Owned Mobile Device Agreement is entered into between the User and AFROHUN LLC (AFROHUN), effective the date this agreement is executed by AFROHUN's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a AFROHUN supported mobile device by the User for AFROHUN business is a privilege granted to the User, by management approval, per the AFROHUN Owned Mobile Device Acceptable Use and Security Policy. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to AFROHUN and to ensure the data remains secure.

In the event of a security breach or threat, AFROHUN reserves the right, without prior notice to the User, to disable or disconnect some or all AFROHUN services related to connection of a AFROHUN owned mobile device to the AFROHUN network.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following AFROHUN policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, AFROHUN Owned Mobile Device Acceptable Use and Security, and other related policies including, but not limited to, Anti- Virus, E-Mail, Network Security, Password, Safeguarding Member Information, Telecommuting.

The User of the AFROHUN owned mobile device shall not remove sensitive information from the AFROHUN network, attack AFROHUN assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

AFROHUN will offer the following support for the AFROHUN owned mobile device: connectivity to AFROHUN servers, including email and calendar, and security services, including policy management, password management, and decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), and carrier network or system outages that result in a failure of connectivity to the AFROHUN network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the AFROHUN network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data or which render the mobile device inoperable.

_____

Device Make/Model

_____ _____

User Date

_____ _____

IT Department Management Date