# Acceptable Use Policy



**Author:** Franklin Ochieng Okech

**Date:** 16th July 2018

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Review History** | | | | |
| **Name** | **Department** | **Role/Position** | **Date approved** | **Signature** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Approval History** | | | | |
| **Name** | **Department** | **Role/Position** | **Date approved** | **Signature** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at ICT Authority  in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

ICT Authority provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with the Authority’s policies and protects the Authority against damaging legal issues.

## Scope

All employees, contractors, consultants, temporary and other workers at ICT Authority, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by ICT Authority, or to devices that connect to the ICT Authority’s  network or reside at a ICT Authority  site. The policy addresses the following important ICT objects that includes General requirements, user credentials, computing assets, network usage and electronic communication

## Policy Statement

### General Requirements

#### You shall be responsible for exercising good judgment regarding appropriate use of ICT Authority’s resources in accordance with ICT Authority’s policies, standards, and guidelines. ICT Authority’s resources such as user credentials, computing assets, network and all electronic communication assets may not be used for any unlawful or prohibited purpose.

### User Accounts

#### You shall be responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

#### You shall maintain all user credentials in accordance with the Password Policy.

#### You shall ensure through legal or technical means that proprietary information remains within the control of ICT Authority at all times. Conducting ICT Authority’s business that results in the storage of proprietary information on personal or non- ICT Authority controlled environments, including devices maintained by a third party with whom ICT Authority does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by ICT Authority, or its customer and partners, for the Authority’s business.

### Computing Assets

#### You shall be responsible for ensuring the protection of assigned ICT Authority’s assets that includes the use of computer cable locks and other security devices. Laptops left at ICT Authority overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of ICT Authority assets to the security department.

#### You shall ensure all PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to reasonably minutes. You shall ensure that you lock the screen or log off when the device is unattended.

#### Devices that connect to the ICT Authority network shall comply with the Minimum Access Policy.

#### You shall not interfere with corporate device management or security system software, including, but not limited to, antivirus, firewalls and intrusion detection systems.

### Network Use

You are responsible for the security and appropriate use of ICT Authority’s network resources under your control. Using ICT Authority’s resources for the following is strictly prohibited:

#### You shall not cause a security breach to either ICT Authority’s or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

#### You shall not cause a disruption of service to either ICT Authority’s or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

#### You shall not introduce honeypots, honeynets, or similar technology on the ICT Authority’s network.

#### You shall not violate copyright laws, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

#### You shall not export or import software, technical information, encryption software, or technology in violation of international or regional export control laws.

#### You shall not use the Internet or ICT Authority’s network that violates the ICT Authority’s policies, or local laws.

#### You shall not Intentionally introduce malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

#### You shall not use port scanning or security scanning on a production network unless authorized in advance by Information Security department.

### Electronic Communications

The following are strictly prohibited:

#### You shall not inappropriately use the communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates ICT Authority policies against harassment or the safeguarding of confidential or proprietary information.

#### You shall not send spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

#### You shall not forge, misrepresent, obscure, suppress, or replace a user identity on any electronic communication to mislead the recipient about the sender.

#### You shall not post the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

#### You shall not use the ICT Authority e-mail or IP address to engage in conduct that violates ICT Authority’s policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with an ICT Authority’s e-mail or IP address represents ICT Authority to the public; therefore, you shall exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the Authority.

## References

[Computer Misuse and Cybercrimes Act of 2017](./Computer%20Misuse%20&%20Cybercrimes%20Act.pdf)

[Data Protection Bill Of 2012](DATA_PROTECTION_BILL_FROM_AG_for_publication_to_Parliament.pdf)

[ICT Authority Information Security Standard of First Edition 2016](./Information%20Security%20Standards.pdf)

[Kenya Information and Communication Act of 2013](Kenya_Information_and_Communications_Act.pdf)

[National ICT Policy of 2016](National-ICT-Policy-20June2016.pdf)

[National ICT Masterplan of 2017](./THE%20NATIONAL%20ICT%20MASTERPLAN%202017.pdf)

[ICT Authority Stratergic Plan 2013-2018](./ICT%20Authority%20Strategic%20Plan.pdf)

[National Cybersecrurity Strategy of 2014](./NATIONAL%20CYBERSECURITY%20STRATEGY.pdf)

[NIST Cybersecurity Framework 2016](./Framework%20for%20Improving%20Critical%20Infrastructure%20Cybersecurity,%20Version%201.1.pdf)

[NIST Policy on Information Technology Resources Access and Use](./NIST%20Policy%20on%C2%A0Information%20Technology%20Resources%20Access%20and%20Use%20_%20NIST.pdf)

[FBI Acceptable Use Policy Framework](./FBI%20Acceptable%20Use%20Policy.pdf)

## Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and possible criminal prosecution. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with ICT Authority.

## Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **honeypot, honeynet** | Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities. |
| **Spam** | Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant. |

## Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| 16th July 2018 | Franklin Ochieng | Policy created |
| 24th July, 2018 | Franklin Ochieng | First Draft, made changes to the tone of the policy |