2013

ICT POLICY DOCUMENT

The ICT policy document sets out guidelines that governs ownership, accessibility and usage of Information technology equipment, information and services that are under the management of the Dispensers for Safe water organization

Table of Contents

Definition of Terms

The following terms and acronyms are used consistently in the document and below is their meaning as per the context of this document

DSW – Dispensers for Safe water

Asset - Any property/equipment owned by DSW

Devices – Any electronic equipment used by DSW to handle data and ICT related operations. Examples include: Smartphones, Laptops, Tablets, Servers, storage Media (flash-disks, portable hard drives, CD ROMs

IS – Information system. This is a an equipment (a group of equipment) or software that handles data input, processes it to output information or store it electronically for later retrieval

IPA – Innovations For Poverty Action. The usage of the term may be taken to mean Evidence Action in some cases

Systems Administrator – A person in charge of a software or application that is used in DSW operations

Network Administrator – The person in charge of the DSW network connectivity. This shall be the IPA IT coordinator (in Kenya) or the IS officers for the other countries

Data/information – Important facts and figures collected as part of the DSW daily operations

Virus – A software program which when gets access to an information system/device causes harmful effects such data loss or malfunctioning of the device

Anti-virus – A software program created to detect, destroy, counteract or mitigate the virus and its effects on an information system

Firewall - A firewall is a set of related programs, located at a network , that protects the resources of a private network from users from other networks.

Malicious code – Any software program created with an intention to cause damage to any existing information system or data

1 Introduction

1.1. Background

The Dispensers for Safe water organization (DSW) supports the development and provision of information and communication tools and systems that facilitate and enhance the management of its operations.

Information management and information technology management are vital in the delivery of organization programs and, when planned and managed properly, would improve service delivery, increase productivity and reduce costs to the organization.

1.2. Policy formulation

The formulation and enforcement of information technology and security policies will enhance the performance of the organization in delivering, implementing, and maintaining Devices, software, hardware and networks suitable to the organizational needs, as well as its collaborating organizations with which DSW shares information.

The policy defines the duties and responsibilities of the DSW Employees, who use devices, Network, Software and hardware systems in performance of their duties.

1.3. Scope

The Information technology policies cover the organization's management of the acquisition use and disposal of electronic resources, including software, hardware devices, data and network systems.

This policy applies to all Employees of the organization, contractors and consultants, including all personnel affiliated with the organization whether at the company's premises or elsewhere.

The policies also apply to all equipment that is owned or leased by the organizations which are essential resources for accomplishing the organization's strategies and objectives. These resources are valuable organization assets to be used and managed responsibly to ensure their integrity, security and availability for appropriate organizational activities. All authorized users of these resources are required to use them in an effective, efficient and responsible manner. Users must be aware of user rights and responsibilities, which outline liability for personal communication, privacy and security issues and consequences of violations.

1.4. Purpose

The purpose of this policy is to ensure the responsible use, availability, confidentiality and integrity of Information Technology systems that support all the activities of the organization. Effective security will be

achieved by working with proper discipline, in compliance with Organizational Policies and legislation, and by adherence to approved Organization procedures and standards.

1.5. Objectives

The ICT policy document is developed to achieve the following objectives. It hereby undertakes to:

i. provide a policy framework within which the organization can derive the maximum benefits from the use of information technology
ii. Provide suitable hardware and software systems that guarantee information security, secure environment and safe working practice in the operation of the equipment;
iii. Ensure that users are aware of and fully comply with the Information Technology and Security policies, procedures, guidelines, standards and relevant legislation to achieve best value in Information Technology provision;
iv. Ensure that the organization plays an active and responsible part in the wider use of Information and Communications Technology (ICT).
v. Ensure that all users understand their responsibilities in protecting the data and equipment that they handle.

1.6. Responsibilities

The Information systems manager and information systems officers shall be responsible for the following:

- ✓ Initiating and drafting Information Technology and security policies and for arranging the approval process as appropriate for each policy.
- ✓ Maintaining Information Technology policy in an up-to-date and in an accessible form.
- ✓ Arranging the dissemination of Information Technology policy in an appropriate and accessible way.

Each Employee, contractor, consultants, and all personnel affiliated with the organization shall be responsible for the following:

- ✓ Understanding and complying with Information Technology and security policies.
- ✓ Reporting to authorities any breach of the laid down policies

.

1.7. Policy Awareness

All Information technology and Security policies, guidelines, procedures and standards, will be made freely available electronically on the company's Web server to all Employees and will form the up-to-date official version. Anyone responsible for authorizing the use of facilities within the scope of these policies shall be responsible for informing new users.

1.8. Changes to the Policy

The normal process for changing Information Technology Policy will be for a request to be made to the Information systems Manager who will arrange for review of the requested changes with the Information systems officers and thereafter the country program director. After approval the Information policy will change and be published on the web server.

In the event of a need for urgent change, this may be approved by the program director.

1.9. Enforcement

The Information systems team and the respective area coordinators shall conduct quarterly audits to ensure that the policies are followed. Disciplinary action shall be taken against those employees who violate the regulations according to the decision that shall be arrived at by the Human Resources department in consultation with the DSW IS team, DSW management, area coordinator in charge and HR department.

1.9.1 Classification of offences and penalties:

#	Class	Description	Example	Penalty
1	Minor	Petty ICT offences which can happen due to ignorance of ICT policy	Unauthorized repair of ICT equipment	Issuance of Warning letter
2	Major	Offences which occur due to deliberate negligence of the ICT policy guidelines	Vandalizing or Losing ICT property,	payment of a fine
3	Grave	Very serious offences which are committed deliberately with an aim of sabotaging organization operations	Hacking into the server, Deliberate deletion of data	Termination of contract

2 Access control policy

2.1 Purpose

Access control policy is put in place to protect DSW information by controlling who has the rights to use different information resources and by guarding against unauthorized use. It regulates who can access DSW information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing DSW information in any format, and on any device.

2.2 Passwords Policy

2.2.1. Choosing passwords:

Passwords are an integral form of defense for information systems and together with user ID help to authenticate users. A poorly chosen or misused password poses a security threat. A strong password consisting of a mixture of letters, numerals and special characters is recommended over a weak one.

2.2.2 Protecting passwords:

The passwords must be protected at all times. The following guidelines must be adhered to in order to effectively protect the passwords:-

- ✓ Never reveal your password to anyone.
- ✓ Never store your passwords in an open place or a place open to theft.
- ✓ Do not use the same password to access different systems.
- ✓ Default passwords must be immediately changed.
- ✓ Once the user suspects or discovers that their password has become known to someone else, it must be changed immediately.
- ✓ Administrators and users must use strong password(s)

2.3 DSW Information Systems User registration

A request for access to DSW's network systems and data must first be submitted to the system administrator for approval.

Applications for access must only be submitted if approval has been gained from the system administrator.

When an employee leaves DSW, their access to the network systems and data MUST be suspended on their exit. This must be indicated on the employee's clearance form as issued by the HR. It is the responsibility of the system administrator to suspend the access rights

2.4 User's responsibilities

It is the user's responsibility to ensure that their user ID and password are not used to gain unauthorized access to a system by:-

- ✓ Following the outlined password control policy.
- ✓ Ensuring that their devices while not in use or left unattended is locked or logged out.
- ✓ Leaving nothing on display that may contain information such as login names and passwords.

2.5 User authentication for external connections

This applies to situations where an authorized IS user might require access to DSW information systems access from remote locations

- ✓ Where remote access to the DSW network is required, an application must be made through the system administrator.
- ✓ Remote access to the network must be secured by two factor authentication consisting of a username and password.

3 Information / Data security Policy

3.1 Introduction

Data is considered a primary asset and as such must be handled, used and protected in a manner commensurate to its value.

3. 2 Data life cycle

The typical life cycle of data is: generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data.

Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access.

Data must only be used in a manner consistent with this policy.

In conformance with this policy only uniquely identified, authenticated and authorized users are allowed to access data.

3.3 Classification of information/data

(i) **Sensitive**: This is highly sensitive information that could seriously damage the organization existence and reputation if such information were lost or made public. Examples include: includes financials, internal audits and internal evaluation

(ii) **Confidential:** Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations. Confidential Information would include: accounting information, Employee evaluation and appraisal information.

(iii) **Private information:** Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include: internal memos and minutes of meeting, research data, monitoring and evaluation data.

(iv) Public information: This is Information in the public domain which has been approved for view by the public. This information can be shared to anyone. Examples include: program success stories

.

4 Internet and Email Policy

4.1 Internet

Internet connectivity, maintenance and fair usage auditing are the roles of the network administrator. It is the responsibility of internet users to ensure compliance with this policy and to exercise their own best judgment on the matter when using the internet.

4.1.1 Setting up Internet Access

The network administrator is responsible for setting up Internet access are to ensure that the company's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured anti-virus program.

4.1.2 Downloading Files and Information from the Internet

Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material. Internet users are encouraged to download only the material which has direct program relevance and only from trusted websites.

4.1.3 Using Internet for Work Purposes

The network administrator is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security incidents. The network administrator shall implement restrictions on network equipment to block access to sites deemed inappropriate

4.1.4 Giving Information when Ordering Goods on Internet

Employees authorized to make payment by credit card for goods ordered on the Internet, are responsible for its safety and appropriate use.

4.1.5 Filtering Inappropriate Material from the Internet

The Organization shall use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by Employees.

The network administrator has the right to utilize software that makes it possible to identify and block access to Internet sites containing explicit or other material deemed inappropriate in the workplace.

5 Web Policy and E-mail policy

5.1 Organization Web Sites

Due to the significant risk of malicious intrusion from unauthorized external persons, administrative access shall be limited to authorized personnel.

The Web sites are important information resources for the organization and their safety from unauthorized intrusion is a top priority.

5.2 Email Usage Policy

I. The electronic mail system hardware is IPA property. Additionally, all messages composed, sent, or received on the electronic mail system are and remain the property of IPA. They are not the private property of any employee.

II. The use of the electronic mail system is reserved solely for the conduct of business at DSW. It may not be used for personal business. Occasional personal use, which does not interfere with the employee's job performance, is acceptable, but such use remains subject to all provisions of this policy. Employees are advised to create a separate e-mail address for personal communications.

III. The electronic mail system may not be used to solicit for commercial ventures or political or religious causes, outside organizations, or other non-job-related solicitations.

IV. The electronic mail system is not to be used to create, send or forward messages which are obscene, pornographic, defamatory, harassing, threatening, contain racial or sexual slurs, or which are otherwise inappropriate in the context of the organization's ethos and core values. ("Chain Letters" would be regarded as inappropriate electronic mail).

V. The electronic mail system shall not be used to violate copyrights or other proprietary rights by distributing unauthorized copies of materials owned by others, nor shall it be used to distribute confidential or proprietary DSW materials without proper authorization.

VI. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

VII. The attachment of data files to a mail shall only be permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.

VIII. Incoming e-mail shall be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code.

6 Network Security

6.1 Network Management policy

I. Relocation, changes and other reconfigurations of network access points and devices will only be carried out by network Administrators according to procedures laid down by them.

II. The implementation of new equipment or upgraded network software or hardware must be carefully planned tested and managed by the network management team.

6.2 Network design and configuration policy

I. The network must be designed and configured to deliver levels of performance, security and reliability suitable for the DSW's organizational needs, whilst providing a high degree of control over access.

II. Access controls and routing should be used to prevent unauthorized access to network resources and unnecessary traffic flows between domains.

III. Appropriately configured firewalls should be used to help protect the DSW's critical organization systems.

IV. No changes to the network infrastructure, such as the introduction of a router or switch, may be undertaken without approval in advance by the Network administrator.

6.3 Connecting devices to the network

I. Privately owned network devices may only be connected to the DSW network in special circumstances approved by the Network administrator. Privately or DSW owned laptops/PCs can be connected to the wireless network.

II. All devices whether privately owned, or owned by other organizations, must meet DSW network connection standards and their usage must conform to DSW Security policy

III. Network administrators have the right to inspect the configuration, test security and monitor network traffic for all devices connected to DSW-Networks in accordance with normal operational network management procedures.

IV. Every device connected to the network must be associated with a contactable person responsible for its administration and must be actively maintained.

V. Where applicable, network devices should have current and automatically updated anti-virus software installed. Employees in possession of devices should alert the system administrator 3 months in advance if any of the installed software is near expiry.

VI. Where applicable, network devices should have correctly configured firewall software installed. As a default all ports should be closed unless specifically opened.

6.4 Network termination or restrictions

I. The organization shall terminate or restrict the network connection without notice whenever a LAN, a network device or a user poses any security risk to the company network equipment, software and data.

II. If there is any doubt as to whether some intended usage of the network is permitted, or could significantly impact performance of the network, then advice should be sought from the Network Administrator before proceeding.

III. Network monitors and similar devices which allow the inspection of network traffic must not be used without the prior approval of the network administrator.

7. DSW Software

This section of the policy governs the acquisition, development, ownership and licensing of software in use at DSW organization

7.1 Software acquisition

I. When software for use by the DSW is being procured there must be an assessment of whether the software incorporates adequate security controls for its intended purpose.

II. It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.

III. During procurement of software, the procurement policy will apply and it may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.

7.2 Software development and Ownership

I. All software acquired for or on behalf of the organization or developed by company employees or contract personnel on behalf of the organization shall at all times shall remain organization property. All such software must be used in compliance with applicable licenses, notices, contracts and agreements.

II. Software developed at DSW must be assessed by the IS team for its potential to introduce information security risks and any such risks must be adequately addressed.

III. Upgrades or other changes to locally developed software must be assessed by the IS team for any risks to information security.

7.3 Software installation, regulation and usage

I. For each item of software owned and managed by the organization a master copy of any media, enabling codes and installation instruction must be stored safely in accordance with the organizational procedures.

II. Use of illegal software and using software for illegal activities could be construed to be gross misconduct.

III. Use of software which tests or attempts to break DSW system or network security is prohibited unless the Network Administrators have been notified and given authorization for the purpose of penetration testing.

IV. Use of software which causes operational problems to the network platforms, or which makes demands on resources which are excessive or cannot be justified is prohibited.

V. Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service.

VI. When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software and data stored on it.

8 Physical Security

Physical security measures are steps that DSW will take to manage physical access to an information resource. DSW considers physical security as the first line of defense against theft, sabotage, and natural disasters. Examples of measures that DSW will undertake include restrictions on entry to equipment areas, locking, disabling, or disconnecting equipment;

8.1 General physical security

I. To ensure protection of all information assets the information technology department shall maintain an inventory of information systems. This inventory should indicate all existing hardware software, databases, and data communication links.

II. Each individual that is granted access rights to an Information Resources must receive emergency procedures training for the resource where and when necessary.

III. Requests for access must come from the applicable information systems officer.

8.2 Equipment Security

This section applies to all Employees of the DSW, contractual third parties and agents of DSW who use DSW IT facilities and equipment, or have access to, or custody of DSW devices.

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the DSW's systems and the information that they use or manipulate.

An Information Security Incident includes, but is not restricted to, the following:

I. The loss or theft of data or information.

II. The transfer of data or information to those who are not entitled to receive that information.

III. Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.

IV. Changes to information or data or system hardware, firmware, or software characteristics without DSW's knowledge, instruction, or consent.

V. Unwanted disruption or denial of service to a system.

VI. The unauthorized use of a system for the processing or storage of data by any person.

9.0 DSW Asset Ownership, protection and hand-over

9.1 Loss of DSW ICT equipment's

DSW invests a lot of financial resources in the acquisition, distribution and maintenance of Information system equipment. All employees allocated DSW ICT property must take utmost good care of the property failure to which a punitive measure may be taken. The Area coordinators in a given area are responsible for the overall quality and security of equipment in areas they manage.

In the event of asset loss due to situations beyond the employees control such as theft, fire damage or any other accidental occurrence the employee should:

I. Report the incidence to a police station

II. Fill in a P3 form indicating the information about the incidence

III. Submit a written report to the procurement department, the area coordinator in charge and the information technology department together with a copy of the P3 form about the incident

9.2 Maintenance and repair

It is the responsibility of the staff member assigned a laptop or smartphone to ensure that it kept in good repair by adhering to good computer and smartphone practices. This means that the assigned staff member must keep the device cool and dust-free, and protected with a soft case.

Laptop maintenance shall be done every six months, and is the responsibility of the IS team. Maintenance includes virus and malware scans, deleting unused programs and conducting performance benchmarks.

If an electronic device requires repair, the staff member must alert the IS Officer promptly, who will then forward it for repair through the IPA country office.

9.2 Employee asset liability matrix (in case of equipment loss)

In the event of loss of DSW ICT equipment due to employee negligence the following compensation shall be effective within an agreed time period:

I. 100% purchase price for all equipment less than 1 year old.

II. 75% purchase price for all equipment more than 1 year old but less than 2 years old.

III. 50% purchase price for all equipment more than 2 years old.

9.3 Disposal of DSW assets

9.3.1. General Disposal guidelines

I. DSW Staff CANNOT purchase phones, laptops and any other ICT equipment from DSW bought with money from donors. For all other phones and laptops the following shall govern all staff purchases.
   a) 100% purchase price for all equipment less than 1 year old.
   b) 75% purchase price for all equipment more than 1 year old but less than 2 years old.
   c) 50% purchase price for all equipment more than 2 years old.

   The procurement department shall determine the appropriate time, equipment to be disposed and the process of disposal

II. An Employee who loses DSW equipment during a time when DSW equipment is available for sale shall not be allowed to record their loss as a purchase from DSW but shall have to record it as a lost item and compensate Loss of DSW ICT equipment's.

III. All DSW equipment which are not in use, have expired or damaged beyond repair shall be returned to DSW for safe storage and inventory keeping.

9.3.2. Disposal of ICT assets by destruction

The disposal of hardware by destruction may only be carried out with the approval of the IS manager and procurement Officer. Certificate of destruction will created by the IPA country office and the hardware will be disposed of according to the current WEEE (Waste Electrical and Electronic Equipment) regulations. These regulations ensure environmental conservation through the efficient, safe and conservative disposal of electronic waste.

9.4 Handing over of DSW assets

All DSW staff upon completion of their contract are required to submit the DSW ICT equipment under their care to the ICT department as part of the exit clearance process.

Conclusion

All employees, contractors with DSW and users of the DSW ICT assets, data and Networks are expected to read, understand and adopt the use of the ICT policy thought their period with DSW. Clarification of any part of the policy should be sought from the IS manager. Employees, contractors and users of DSW information technology equipment, services or data must exercise their own best judgment of the situation for any situation that might not have been captured in the policy document