Creating value through
inclusive finance

Information and Communication Technology (ICT) Management Policy

Date of revision	Two years after approval
Policy owner	Chief Operating Officer
Status	Public

Version control

Draft	Submitted		Reviewed	Approved
Version 1	ABC-LLP	4 October	20 October 2020	
Version 2	ABC-LLP	5 November	30 November 2020	10 December 2020

Contents of this policy

1. Policy statement

FSD Kenya's Information communication and technologies (ICT) systems are intended to promote effective communication and working practices within the organisation. FSD Kenya will keep all information technology (IT) policies current and relevant.

FSD Kenya information resources must be protected against events that may jeopardise information security by contaminating, damaging, or destroying information resources.

Misuse of ICT systems can be prejudicial to FSD Kenya's activities and its reputation. Breach of this policy may be dealt with under FSD Kenya's disciplinary policy and procedures.

2. Purpose

This policy outlines the minimum standards that must be observed by all staff and consultants when using these systems, the circumstances in which FSD Kenya will monitor the use and the action it will take in respect of breaches of these standards.

This policy further seeks to:

a) Ensure the provision of adequate and reliable information systems

b) Provide guidelines on the usage of ICT software, hardware and services

c) Ensure information security of FSD Kenya systems and data

d) Promote efficient utilisation of information systems by FSD Kenya employees

3. Scope

This policy applies to all FSD Kenya staff and anyone else who, for whatever reason, has access to FSD Kenya's ICT systems. This ICT policy covers all Information Technology (IT) facilities, hardware, software, and services provided by FSD Kenya. These are:

a) **Facilities:** FSD Kenya offices**,** meeting rooms, server room

b) **ICT services** such as ICT support in software, hardware and any other computing infrastructure and technical support to FSD Kenya staff.

c) **Hardware** such as personal computers (PCs), laptops, servers, printers, scanners, network routers and switches, power backup equipment (e.g. uninterruptable power backup/ supplies - UPS), LCD projectors, cameras (digital and camcorders), PDAs, smartphones and other mobile computing devices, flash-disks/external hard-disks, Private Automatic Branch Exchange (PABXs), telephone heads, fax and photocopiers, and all other ICT related hardware.

d) **Software** such as PC operating systems, antivirus software, Microsoft Office 365, enterprise planning resource (ERP) solution, cloud platform, servers' operating systems and applications on Microsoft Azure, FSD Kenya website, On-Prem server and database systems, and any application software acquired by FSD Kenya.

4. ICT facilities usage policy

All ICT assets owned by FSD Kenya will be issued to its staff for official use through the ICT support team. The ICT support team will be the custodian of ICT systems, including software, and hardware as a measure to facilitate standardisation.

FSD Kenya will avail hardware, software, and systems relevant to the staff's work requirements. Staff must take utmost care of such facilities and ensure responsible and secure usage.

Users shall not relocate, repair, reconfigure, modify ICT equipment, or attach external devices other than explicitly authorised data storage devices to such equipment without the authority from the ICT support team.

FSD Kenya may authorise staff to use external disks to store official information. These external disks must adhere to FSD Kenya security standards such as be password protected, encrypted, scanned for viruses and other harmful software.

5. ICT equipment maintenance policy

ICT Support shall ensure that all ICT equipment is always kept in proper working condition.

All ICT equipment shall be maintained in accordance with the procedure for ICT equipment maintenance.

In areas where FSD Kenya has no adequate internal capacity, annual maintenance contracts will be entered into with service providers.

6. Internal ICT support policy

While FSD Kenya will strive to provide ICT support services, staff assigned ICT equipment must ensure they are not exposed to risks that can cause equipment damage.

ICT Helpdesk Officers shall be available to offer technical support on any software or hardware upon users' requests.

For equipment authorised to be used out of office, the responsible staff must exercise due care.

7. Out-sourced ICT services policy

FSD Kenya shall out-source ICT equipment or services whenever such capacity lacks within with approval from the management upon recommendation from the Procurement Officer. Such a need shall be supported by a need's assessment report from the Procurement Officer

All out-sourced ICT equipment and services will be supervised by Procurement Officer in accordance with Service Level Agreements (SLAs) that are in place.

The out-sourced services shall be based on annual contracts that may be renewed based on recommendations from the Procurement Officer.

8. System controls and information security policy

The ICT systems, and the service they provide, will be protected by effective control of security risks at all levels of the organisation, providing, managing, and operating to ensure that the requirements regarding availability, confidentiality and integrity are preserved.

Access to the systems will be restricted to authorised users as determined by the COO.

Anyone who is not authorised to access the FSD Kenya network should only be allowed to use terminals under supervision.

Staff must lock their terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in their absence.

The IT team will advise on the introduction of enhanced measures for specific groups and will support several specific information security services.

9. Physical security

ICT resources are generally exposed to the risk of unauthorised access, manipulation, disruption, and natural disasters.

To protect the ICT equipment and systems and ensure their availability, FSD Kenya has put in place appropriate physical control measures to ensure that its ICT resources are safeguarded.

Appropriate physical controls have been established to limit access to ICT infrastructure, computer equipment and data, commensurate with the acceptable level of risk.

Third parties may enter FSD Kenya premises only when given an appropriate security authorisation and may enter areas of the premises commensurate with their function.

Third parties given entry into high security areas (e.g., server room) should be accompanied by FSD Kenya staff

10. Password policy

The password policy establishes a standard for the creation of strong passwords and the protection of those passwords.

All user-level and system-level passwords must conform to the Password Construction Guidelines defined in the ICT manual.

Passwords must be changed every 60 days and not shared with anyone, including supervisors and co-workers.

Passwords must not be shared with anyone including colleagues and supervisors.

Passwords shall not be written down, physically stored anywhere in the office or sent electronically.

11. Data security

FSD Kenya shall develop rules, regulations and guidelines that ensure confidentiality, integrity, availability, and safety of all organisation information.

Users shall be given the minimum access to sensitive information or key operational services necessary for their role.

Access shall be removed when individuals leave their role or the organisation. Periodic reviews should also take place to ensure appropriate access is maintained.

12. Copyright and license agreements

Only licensed software shall be used in FSD Kenya. Copying and distribution should not be done without the necessary licenses. The ICT support team will ensure that all software applications used by staff comply with the relevant licensing agreements, compile them and maintain a record.

FSD Kenya owns or possesses adequate rights or licenses to use all material trademark and data that is generated in its operations.

13. Internet usage policy

To ensure productive, appropriate use and to minimise risks, users shall use the internet in an effective, ethical and a lawful manner.

Users shall not use the organisation's internet access to view, print, distribute, display, send or receive images, text, or graphics of offensive or obscene material or material that violates any Kenyan law or breaches any FSD Kenya's policies.

FSD Kenya shall maintain a log of sites visited as a means of determining appropriate usage. This will be in line with the data protection policy.

FSD Kenya shall install and maintain firewalls to filter content coming in or going out via the internet and protecting against external attacks.

14. Email policy

FSD Kenya encourages the use of email and respects the privacy of users. FSD Kenya will not routinely inspect, monitor or disclose the contents of an email without the consent of the user. However, subject to the requirements for authorisation, notification, and other conditions specified in this policy, FSD Kenya may inspect, monitor, or disclose email when it believes that it has a business need to do so.

Staff will be issued with official standardised email addresses. All official email communications shall be through official email addresses. ICT Support will ensure that mail service is available to staff always.

Email users shall avoid broadcast communication (i.e. send to large groups of people using email aliases) unless where necessary. One must always ensure proper audience segregation is used before sending an email.

FSD Kenya mail service shall not be used to broadcast other unofficial information or requests (e.g., information or opinions on political matters, social matters, and personal requests for information etc.) The use of email shall be related to FSD Kenya's activities.

15. Website policy

The Communications Manager shall ensure that the FSD Kenya Website(s) is always kept in an updated status. The website shall be maintained in a user friendly and accessible state.

All requests for changes on the website shall be subject to the approval of the COO.

The ICT Section shall ensure that the website is always available to the public.

16. Acquisition and disposal of ICT Facilities policy

Information asset equipment - comprises computers, servers, laptops, tablets, mobile phones, solid-state drives, external hard drives, server/computer backups on tape or disk, USB sticks, scanners, printers, and CDs/DVDs. Conferencing facilities such as TVs, cameras, audio and Visio equipment are also information assets.

a) Acquisition of ICT facilities

The procurement policy shall guide acquisition of ICT facilities. Where funds are donated from external sources, the respective donor's conditionality's, terms, agreements, or memoranda of understanding shall apply.

All user requests for acquisition of items of ICT nature shall be channelled through the ICT support who will confirm lack or availability of such items. If not available, ICT support will prepare specifications and forward the request to the procurement officer.

ICT support team shall ensure that all software licenses in use by FSD Kenya are promptly renewed to guarantee smooth operations and continuous software updates and support from manufacturers.

b) Disposal

ICT Support shall identify hardware and software to be disposed of and liaise with the Procurement and finance teams for assessment leading to disposal as per the disposal policy and authorisation of the P&P.

ICT Support shall ensure that all equipment earmarked for disposal is cleared of FSD Kenya's data and storage media destroyed.

17. Enforcement and control

Unauthorised access to information facility or computer (including workstations and PCs) over the network or to modify its contents is strictly forbidden.

Staff within FSD Kenya network shall not write, publish, browse, bookmark, access or download obscene, pornographic or paedophilia materials.

All hardware, software, or systems in use by FSD Kenya shall be licensed.

Deliberate breach of this policy statement may lead to disciplinary measures in accordance with FSD Kenya disciplinary policy. These may include but not limited to being denied access to computing facilities or surcharge for the loss or abuse of ICT facilities or services and where applicable law enforcement agencies may be contacted where a breach constitutes a criminal offense.

Where third parties are involved in the breach of this policy, it may also constitute a breach of contract.

FSD Kenya reserves its right to conduct forensic investigations on Staff laptops in case of suspicious use/practices.

18. Privacy and confidentiality

FSD Kenya shall guarantee the right to privacy and confidentiality of staff information while discharging ICT services.

Information/services/resources available within IT facilities will not be used to monitor the activity of individual staff in anyway without their prior knowledge. This shall not be applicable in the following cases:

a) In the case of a specific allegation of misconduct or for any other investigation purpose, FSD Kenya may authorise access to such information or denial of service while the staff is under investigation.

b) Where the ICT Section or any other section cannot avoid accessing such information whilst administering, resolving ICT systems problems or in their day-to-day work activities

19. Bring your own devices (BYOD)

FSD Kenya grants its employees the privilege of using smartphones and tablets of their choosing at work for their convenience. FSD Kenya reserves the right to revoke this privilege if users do not abide by this policy and associated procedures.

All employees must follow the Data security policies and procedures when working on company data from their personal devices.

20. Change management

Change management is the process that controls the life cycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

FSD Kenya's technology environments will be managed through an established process. FSD Kenya will utilise the best practice framework (e.g., Information Technology Infrastructure Library [ITIL]) for the implementation of change management within its technology environments.

FSD Kenya IT must use the current tool and documented change management process to prioritise, control, and approve all technology solution changes.

21. Security incident reporting and management

The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the FSD Kenya's network. Some examples of security incidents are:

a. Illegal access to FSD Kenya's computer system. For example, a hacker logs onto a production server and copies the password file.
b. Damage to FSD Kenya's computer system or network caused by illegal access.
c. Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
d. Malicious use of system resources to launch an attack against another computer outside of the company network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Staff, who believes their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the **Chief Operating Officer** immediately.

Staff shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

Security incident management measures will include:

a) Information security incident identification.

b) Incident prevention, reporting, response, and containment.

All personnel must adhere to the incident prevention, reporting, and containment guidelines to ensure adequate protection of FSD Kenya information resources.

22. Business continuity

FSD Kenya will ensure service continuity through the alignment of Business Continuity Plans and Disaster Recovery Plans to prepare for, respond to, and recover from any event that disrupts, or threatens to disrupt normal operations.

FSD Kenya will ensure that initiatives are in place to appropriately identify all environments and the associated data that require backup procedures to aid in disaster recovery.

23. Roles and responsibilities

The Programme investment committee (PIC) has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to the **ICT function.**

FSD Kenya ICT function has the added responsibility for reviewing the specific sets of controls to support this policy, taking account of changes in the internal and external environments and the FSD Kenya's risk appetite.

Chief operations officer and the Chief executive officer have the managerial oversight of this policy

Heads of FSD Kenya functions and **projects** are also responsible for ensuring that staff are aware of the need to adhere to this policy and report non-compliance to FSD Kenya management.

Staff are responsible for adhering to the requirements of this policy. Staff are responsible for the security of any computer terminal used by them and for reporting incidences in line with the process set out in this policy.

Third parties who handle FSD Kenya information are responsible for complying with controls equivalent to those applicable to FSD Kenya managed devices. The requirements of this policy shall form part of the contractual obligations.

Research groups/consultants may have enhanced requirements as a result of the information security requirements of their external partners.

24. Review of this policy

FSD Kenya reserves the right to amend this policy from time to time.

The Chief Operating Officer is responsible for reviewing and updating this policy to ensure that the business and technology changes are aligned with the plan.

A revised copy of the policy will be issued and distributed biennially or when changes are made.

25. Related Policies

a) ICT Manual
b) Human Resources Policy
c) Procurement policy
d) Business continuity and recovery plan
e) Data protection policy