

# **THE REPUBLIC OF LIBERIA**



**Ministry of Finance**

# **IT SECURITY POLICY - IFMIS**

**Version 1.2 – June 2009**

# TABLE OF CONTENTS

Acronyms.....	5
Definitions .....	6
1.0 INTRODUCTION .....	8
1.1 Purpose .....	8
1.2 Objectives.....	9
1.3 Scope .....	9
1.4 Internal Security Management .....	9
1.5 Statement of Responsibilities.....	10
1.6 User Roles and Responsibilities .....	11
1.7 Violation of Policy .....	15
1.8 Acceptable Use Policy .....	16
1.9 Unacceptable Use Policy .....	16
1.10 IT Security Organizational Structure .....	16
1.11 Central Security Group .....	16
1.12 Personnel Policies .....	17
1.13 Process Approach .....	17
1.14 Responsibility of Assets.....	17
1.15 Information Classification .....	18
1.16 IT Security Awareness .....	18
2.0 IFMIS TECHNICAL POLICIES .....	18
2.1 User Names and Passwords .....	18
2.2 IFMIS Network .....	19
2.3 Security Administration .....	20

2.4	Testing and Training .....	20
2.5	Physical Security .....	20
2.6	Equipment Security .....	21
2.7	Operational Procedures & Change Management .....	21
2.8	Information Systems Procurement .....	22
2.9	Valid and Review Dates .....	22
2.10	Security Incident Management .....	22
2.10.1	Incident Reporting .....	23
2.10.2	Incident Recording .....	25
2.10.3	Incident Response .....	26
2.10.4	Information Security Incidents .....	26
3.0	IFMIS ADMINISTRATION POLICIES .....	26
3.1	IFMIS System Administration .....	26
3.2	Securing IFMIS Data .....	27
3.3	Access to IFMIS Information Systems .....	28
3.4	System Log & Audit Trails .....	29
3.5	Licenses .....	30
3.6	Securing Hardware, Peripherals .....	30
3.7	Network Access Control .....	30
3.8	Network Security Management .....	31
3.9	Server Security Policy .....	31
3.10	Virus Prevention And Detection .....	32
3.11	IFMIS Systems Audit .....	32
3.12	Fraud And Cyber Crime Policy .....	33

4.0	BUSINESS CONTINUITY PLANNING.....	33
4.1	IFMIS Backup, Recovery And Archiving .....	33
4.2	Disaster Recovery Site (DRS).....	34
4.3	IFMIS Interconnection Policies.....	34
4.4	Risk Assessment .....	35
5.0	ELECTRONIC FUNDS TRANSFER (EFT) .....	35
5.1	Non Disclosure of Information .....	36
5.2	Right to Feedback .....	36
5.3	Business Day .....	36
5.4	Right to Stop Payment .....	36
5.5	Error Resolution .....	36
5.6	Policy on PGP Keys .....	36
5.7	Policy on SFTP Keys .....	37

APPENDIXIES

APPENDIX I:	Data Center Visitors' Pass.....	38
APPENDIX II:	Adding A New User to the IFMIS System .....	39
APPENDIX III:	Change Request Form .....	40
APPENDIX IV:	Equipment Movement Authorization .....	44

## ACRONYMS

<b>BCP</b>	Business Continuity Plan
<b>DRC</b>	Disaster Recovery Center
<b>EFT</b>	Electronic Funds Transfer
<b>GOL</b>	Government of Liberia
<b>IFMIS</b>	Integrated Financial Management Information System
<b>ISN</b>	Information Sharing Network
<b>ISO</b>	International Standards Organization
<b>IT</b>	Information Technology
<b>ITAP</b>	Information Technology Architecture
<b>MOF</b>	Ministry of Finance
<b>PGP</b>	Pretty Good Privacy
<b>SFTP</b>	Secure File Transfer Protocol
<b>CBL</b>	Central Bank of Liberia
<b>CSA</b>	Civil Service Agency
<b>SLA</b>	Service Level Agreement
<b>ICT</b>	Information Communication Technology
<b>NAT</b>	Network Address Translation
<b>CID</b>	Criminal Investigation Division
<b>DCM</b>	Data Center Manager
<b>GAC</b>	General auditing Commission
<b>GEMAP</b>	Governance and Economic Management Assistance Program
<b>PFM</b>	Public Financial Management

# DEFINITIONS

## 1. Acceptable Use

- a. Information/data and systems may only be used by authorized persons to accomplish tasks related to their jobs. Use of the information systems for personal gain, personal business, or to commit fraud is prohibited.
  
- b. Information not classified as Public document must be protected, and must not be disclosed without authorization. Unauthorized access, manipulation, disclosure, or secondary release of such information constitutes a security breach, and may be grounds for disciplinary action up to and including termination of employment.

## 2. Authorized User

Individual or entity permitted to make use of IFMIS computer or network resources. Some users may be granted additional authorization to access IFMIS data as authorized by the data owner or custodian.

## 3. Data Custodian

Data Custodians are representatives of the IFMIS who are assigned responsibility to serve as a steward of IFMIS data in a particular area. They are responsible for developing procedures for creating, maintaining, and using IFMIS data.

## 4. Information Technology Resources

All IFMIS sites including the data centre, technologies, and information resources used for IFMIS information processing, transfer, storage, and communications. Included in this definition are computers, routers, firewalls, computing and electronic communications devices and services, such as modems, e-mail, networks. This definition is not all inclusive but rather reflects examples of IFMIS equipment, suppliers and services.

## 5. Security Measures

Processes, software, and hardware used by system and network administrators to ensure the confidentiality, integrity, and availability of the information technology resources and data owned by IFMIS and its authorized users. Security measures may include reviewing files for potential or actual policy violations and investigating security-related issues.

## **6. Access Control**

The process of limiting access to the resources of a system only to authorised programs, processes, or other systems.

## **7. Audit Trail**

A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an even in a transaction from its inception to final results.

## **8. Business Owner**

The Deputy Minister for Expenditure and Debt Management, Ministry of Finance.

## **9. Authenticate**

To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

## **10. Authorisation**

The granting of access rights to a user, program, or process.

## **11. Username**

A unique symbol or character string that is used by a system to identify a specific user.

## **12. Password**

A protected, private character string used to authenticate an identity

## **13. Virus**

Computer software that replicates itself and often corrupts computer programs and data.

## 1.0 INTRODUCTION

The Government of Liberia (GoL) has commenced the implementation of an Integrated Financial Management Information Systems (IFMIS). In 2006, the Government of Liberia began to implement wide ranging Public Financial Management (PFM) Reforms under the Governance and Economic Management Assistance Program (GEMAP) that to some extent improved the budget preparation and execution process, enacted a procurement law and prevented the accumulation of domestic arrears. However, the Government of Liberia (GoL) agrees that further deeper reforms are necessary to make the budget management process more effective, establish strong internal controls over budget execution and treasury functions, institutionalize internal audit functions and formalize reporting requirements. In order to improve the public financial management systems, the GoL with the support of the World Bank is implementing an IFMIS that will touch on all financial management process and systems pertaining to public expenditure management. The primary purpose of the IFMIS is to deepen and consolidate reforms in public financial management (PFM) aiming at further strengthening and sustaining accountability and transparency in public financial management, improving governance, and maximizing the Government's efforts towards poverty reduction. It is the desire of the Government, to consolidate efforts in implementing an Integrated Financial Management Information System (IFMIS) that would improve financial management practices for improved public service delivery. It is envisaged that IFMIS will serve as a catalyst towards accelerated PFM Reforms.

The use of IT is vital and must be protected from any form of disruption or loss of service and so it is essential that the availability, integrity and confidentiality of the IT system and data are maintained at a level that is appropriate for IFMIS needs. This IT security policy is based on several international accepted standards such as the ISO 17799, and CobiT and best practices developed by the professional organization like the IFAC, ISO, ISACA, IIA, etc. were considered.

Throughout this IT security policy, reference has been sited to the relevant sections of the information security standards ISO 17799 and IT governance and controls framework CobIT. ISO 17799, also known as BS7799, establishes guidelines for implementing an information security management system. ISO standard 17799 is a set of widely used best practices relating basically to information security. The CobIT is a framework for IT governance and control developed by the information System Audit and Control Association (ISACA) which has gained wide acceptance internationally.

### 1.1 PURPOSE

The purpose of this IT Security Policy is to establish a framework for implementing security and control measures of the computerized information systems in IFMIS.

Recognizing that information provided by the computerized systems is key to the operation of the IFMIS business, it is essential that the information and the infrastructure which supports it is secure from destruction, corruption, unauthorized access and breach of confidentiality whether accidental or deliberate.

## 1.2 OBJECTIVE

The main objective of information security is to provide a trusted environment to protect information assets and preventing and minimizing the impact of security incidents. The below Information security management basic objectives must be maintained at all times:

- 1.2.1 **Confidentiality:** ensuring that the IFMIS data is not disclosed or revealed to un-authorized person.
- 1.2.2 **Integrity:** ensuring consistency of the data, i.e. preventing creation, alteration, or destruction of data.
- 1.2.3 **Availability:** ensuring that the legitimate users are not denied authorized access to resources such as information, computing and communication resources when required.
- 1.2.4 **Authorized use:** ensuring that the IT resources are not used by un-authorized persons.
- 1.2.5 **Non-reputation:** ensuring that one does not deny or alter the information sent across the IFMIS network.

## 1.3 SCOPE

- 1.3.1 This information security policy to all users, computer and networks equipment, Data Center, DRS Site, Hardware & Software and all others which directly or indirectly use or support IFMIS, ITAS, HRMIS and all other Systems services and information.
- 1.3.2. In the event that a combination of circumstances creates doubt about which requirement applies, the most rigorous security protection method will be used.

## 1.4 Internal Security Management

**Objective: To manage information security within IFMIS**

- 1.4.1 **Management commitment to Information Security:** IFMIS management shall actively support the IFMIS through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

- 1.4.2 **Information security coordination:** Information security activities shall be co-ordinated by representatives from Information Security Work-Group of IFMIS with relevant roles and job functions.
- 1.4.3. **Allocation of Information security responsibilities:** All information security responsibilities shall be clearly defined within the user manual.
- 1.4.4. **Authorization Process:** a management authorization process for new information processing facilities shall be defined and implemented.
- 1.4.5 **Confidentiality:** Requirements for confidentiality or non-disclosure agreements reflecting the IFMIS needs for protection of information shall be identified and regularly reviewed.
- 1.4.6. **Contact with special interest groups:** Appropriate contacts with special interest groups or service providers shall be maintained.
- 1.4.7. **Internal review of information security:** The IFMIS approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed internally at planned intervals or when significant changes to security implementation occur.
- 1.4.8 **IFMIS users accessing the system from other sites:** IFMIS users in need of accessing the IFMIS system from a different site shall only be permitted to do so by the Controller from every line Ministry at the very site or confirmation from the IFMIS or from the Manager of the IFMIS system. This is to avoid the possible business risk of unauthorized access of IFMIS resources by officers who have been denied physical access to their offices, for instance when implicated in fraudulent activities.

## 1.5 **STATEMENT OF RESPONSIBILITY IFMIS DC, DRC & SITES**

The protection of all information system resources, such as computer systems hardware, application and systems software, data, documentation, and personnel, is a fundamental responsibility of the Minister of Finance.

**Users:** All users of computer resources on the IFMIS have a responsibility for protecting the security and integrity of information and equipment.

The level of responsibility for management, managers, Application Owners and Users shall be well defined by the business owner.

The IT Administrators shall provide appropriate support and guidance to assist users to fulfil their responsibilities under this policy.

## **1.6 Refer to the User Roles and Responsibilities Manual/documentation**

### **1.6.2 User's Right and Responsibilities**

IFMIS users are granted access to information technology resources in order to facilitate their job activities. However, by using these resources, users agree to abide by all relevant IFMIS policies and procedures, as well as all current laws and in accordance to ISO 17799 standards. These include but are not limited to IT security policies and procedures related to sexual harassment and ethic intimidation harassment, plagiarism, commercial use, security, and unethical conduct, and laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and data privacy laws.

#### **Responsibilities of Users:**

- i. Reviewing, understanding, and complying with all policies, procedures and laws related to access, acceptable use, and security of IFMIS information technology resources;
- ii. Asking system administrators or data custodians for clarification on access and acceptable use issues not specifically addressed in IFMIS policies, rules, standards, guidelines, and procedures; and
- iii. Reporting possible policy violation to the appropriate entities.
- iv. When granted access to the system, ensure that no authority person users it.
- v. User of the system must sign a confidentiality understanding (specimen attached to this policy)

### **1.6.3 Liability for Personal Communications**

Users of the IFMIS information technology resources are responsible for the content of their personal communications. IFMIS management accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

### **1.6.4 Privacy and Security Awareness**

Users should be aware that although IFMIS management has put in place security measures to protect IFMIS computing resources and accounts assigned to individuals, IFMIS management does not guarantee absolute security and privacy. Users shall follow the appropriate security procedures prescribed by management from time to time.

IFMIS assigns responsibility for protecting its resources and data to system administrators and data custodians, who treat the contents of individually

assigned accounts and personal communications as private and do not examine or disclose the content except:

- i. As required for system maintenance including security measures;
- ii. When there exists reason to believe an individual is violating the law or IFMIS policy; and /or
- iii. As permitted by applicable policy or law.

#### **1.6.5 Consequences of Violation**

Access privileges to IFMIS information technology resources will not be denied without cause. If in the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of its IT resources and networks or to protect itself from liability, the Business Owner may temporarily deny access to those resources. Alleged policy violations will be referred to appropriate IFMIS system investigative and disciplinary units. Where an investigation is required, the Business Owner shall appoint an investigative committee comprises of members from GAC, CSA,GSA and MOF. IFMIS may also refer suspected violations of law to appropriate law enforcement agencies. Depending on the nature and severity of the offence, policy violations may result in loss of access privileges, IFMIS disciplinary action, and/or criminal prosecution.

#### **1.6.6 IFMIS Business Owner – Deputy Minister for Expenditure and Debt management**

- i. Authorizes users to have the responsibility and authority for IFMIS resources.
- ii. Establishes and disseminates enforceable rules regarding access controls to and acceptable use of information technology resources.
- iii. Implements security policies and measures to protect data and systems.
- iv. Monitors and manages system resource utilization.
- v. Investigates problems and alleged violations of IFMIS information technology policies.
- vi. Ensure that IFMIS security violations, through the Data Center Manager are brought to the attention of the Business Owner.

#### **1.6.7 IFMIS Rights and Responsibilities**

The Deputy Minister for Expenditure and Debt Management is the business owner and is responsible for taking necessary measures to ensure the integrity and security of the entire system. In case of violation, it is the responsibility of IFMIS business owner to investigate as needed or directed, and to take

necessary actions to protect resources and/or to provide information relevant to an investigation.

#### **1.6.8 Role of the Data Center and Disaster Recovery Center personnel**

- i. Create, disseminate and enforce conditions of use that are consistent with IFMIS-wide policies for the facilities and/or resources under their control.
- ii. Monitor the use of IFMIS resources under their control.
- iii. Investigate problems and alleged violations of IFMIS information technology policies.
- iv. Refer IFMIS violations to appropriate authorities such as the Attorney General for resolution or disciplinary action.
- v. Possible policy violations should be reported to the appropriate persons.

#### **1.6.9 Data Custodians**

- i. Grant authorized users' appropriate access to the data and applications for which they are stewards, working with IFMIS data security and network personnel to limit access to authorized users with a legitimate role-based need.
- ii. Review access rights of authorized users on a regular basis.
- iii. Respond to questions from users relating to the use of system/network resources through Help Desk.
- iv. Implement and oversee processes to retain or purge information according to IFMIS records retention schedules.
- v. Determine the critical levels and sensitivity of the data and/or applications for which they are stewards; determine which IFMIS data is public and private based on IFMIS definitions, in consultation with the IFMIS Project Management.
- vi. Ensure that the security measures and standards are implemented and enforced for the data under their control, in a method consistent with IFMIS policies and sound business practices. The security measures implemented should be based on the critically, sensitive, and public or private nature of the data, and may include methodologies, change management, and operational recovery plans.
- vii. Investigate problems and violations of IFMIS information technology policies.

- viii. Refer violations to the business owner for disciplinary action.

#### **1.6.10 System/Network/Security administrator**

This position should be organizationally independent from IT Administration to avoid conflicts of interest when performing IT security functions.

- i. Take action to ensure the authorized use of the IFMIS resources.
- ii. Provide security of equipment, data, networks, and the communications links.
- iii. Participate and advise as requested in developing conditions of use or authorized use procedures
- iv. Respond to questions from users relating to appropriate use of system/network resources.
- v. Cooperate with appropriate IFMIS personnel and/or law enforcement officials in investigating alleged violations of policy law.
- vi. Maintain the IT Security Policy and ensure all IFMIS users are aware of it.
- vii. Routinely check for improper access rights to IT system.
- viii. Sign off on all major IT program changes, and
- ix. Escalate major IT Security issues and Policy breaches to senior MOF management for resolution.

#### **1.6.11 Information Security Policy**

- i. The IT security policy document shall be approved by management, published and communicated to all employees and relevant external parties.
- ii. The IT security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

#### **1.6.12 Internal Organization**

- i. Management shall actively support security within the IFMIS through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of IT security responsibilities.
- ii. IT security activities shall be coordinated by IT security administrator/person in-charge of network security and representatives

from different parts of the organization with relevant roles and job functions.

## **1.7 Violation of POLICY**

**1.7.1** Violation of IFMIS resources will result in corrective action by management in accordance with GOL policy on Information Management and Security.

**1.7.2** Disciplinary action will be consistent with the severity of the incident, as determined by an investigation and the policy stated in the standing Instructions and Code of Conduct regarding violations.

## **1.8 ACCEPTABLE USE POLICY**

- i. Avoid food, candy or drinks in computer areas.
- ii. Seek permission from the system administrators for assistance to adjust equipment or settings, and report problems immediately.
- iii. Use only your personal account and password, and protect your password.
- iv. Lost, stolen or problems with accounts and passwords should be reported immediately to the IT resources.
- v. Use only software programs licensed and authorized by the IFMIS. Ref to the IT Software Library.
- vi. Accept the responsibility for Internet sites visited, files in your home directory, and all material received under your account.
- vii. Comply with legal and IFMIS restrictions regarding plagiarism and the citation of information resources.
- viii. Work in ways that do not violate the privacy of, nor interfere with, the productivity or other users.
- ix. Email and personal use of computers should not deprive other users of resources required for official duties.
- x. Conserve consumable resources such as stationery.
- xi. Avoid giving out personal information; passwords, name, address etc.
- xii. Log off from the workstation after you have finished, and leave the work area tidy.

## **1.9 UNACCEPTABLE USE POLICY**

USERS are not supposed to use IFMIS IT resources in inappropriate ways that:

- i. Are disruptive or intended to cause problems for other users
- ii. Are illegal or libellous
- iii. Interfere with the normal operations of the IFMIS systems
- iv. Incite hatred or violence
- v. Jeopardize the safety or well being of others
- vi. Encourage the use of drugs/bands substances
- vii. Are pornographic or obscene
- viii. Promote dangerous or antisocial behaviour
- ix. Are threatening or insulting
- x. Would tarnish the reputation of IFMIS

## **1.10 IT SECURITY ORGANIZATIONAL STRUCTURE**

Adequate personnel and resources shall be provided for the IT security policy to function. The GOL shall provide IT Security governance structure. There shall be a Central Security Group established by management, with one of the senior managers as members to give IT security a high profile in the IFMIS organizational charts and job descriptions.

### **1.11 CENTRAL SECURITY GROUP**

This cross functional steering Committee should be chair by senior member of management who is not part of IT Administration. This group should meet at least once a month, have a charter and maintain minutes. The IT security administration will be a key member of this group.

The Group will have the following responsibilities;

- i. Oversee the overall implementation of the IT Security Policy.
- ii. Make recommendation to senior MOF management regarding violation of IT Security Policy.
- iii. Make recommendations to revise the IT Security Policy.

## **1.12 PERSONNEL POLICIES**

- i. The personnel Policy shall be in accordance with the employment guidelines of the CSA
- ii. Only qualified personnel shall be recruited on the IFMIS. Ref to TOR for contracts and job description.
- iii. Activities of users on the IFMIS shall be monitored regularly.
- iv. Background checks and reference verification prior to appointment, code of ethics and obligation shall abide by security practices of IFMIS and should be mentioned in the job description and employment contract.
- v. Users' access rights of persons going on leave and about to be terminated on the IFMIS system shall be disabled temporarily or permanently depending on circumstances the person is away.

## **1.13 PROCESS APPROACH**

This IT security policy is based on ISO 17799 and adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving IFMIS' information security.

The process approach for information security management presented in this policy encourages IFMIS users to emphasize the importance of:

- i. Understanding IFMIS' information security requirements and the need to establish policy and objectives for information security;
- ii. Implementing and operating controls to manage IFMIS' information security risks in the context of IFMIS overall business risks;
- iii. Monitoring and reviewing the performance and effectiveness of the information security management system; and
- iv. Continual improvement based on objective measurement.

## **1.14 RESPONSIBILITY FOR ASSETS**

To achieve and maintain appropriate protection of IFMIS assets

- i. Inventory of assets: All assets shall be clearly identified by being engraved or other forms of identification and an inventory of all assets drawn up and maintained in a fixed assets registry.
- ii. Ownership of assets: All information and assets associated with information processing facilities shall be owned by IFMIS.

- iii. Acceptable use of assets: Rules for acceptable use of information and assets associated with information processing facilities shall be identified, documented and implemented.

## 1.15 INFORMATION CLASSIFICATION

To ensure that information receives an appropriate level of protection.

- i. Information shall be classified in terms of value, legal requirements, sensitivity and criticality to the IFMIS.
- ii. An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by IFMIS.

## 1.16 IT SECURITY AWARENESS

All employees on IFMIS and where relevant, contractors and third party users shall received appropriate awareness training and regular updates in policies and procedures, as relevant for their job function.

## 2.0 IFMIS TECHNICAL POLICIES

### 2.1 USERNAMES AND PASSWORD

- 2.1.1 Scope:** The use of information systems shall be protected by access controls to ensure that only authorized users have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. Therefore all users, vendors and service providers shall require usernames and passwords to access IFMIS computer resources.
- 2.1.2 Super Administrative Access:** The business owner or his designee shall authorize persons to hold such passwords to the IFMIS system.
- 2.1.3 Audit Trails:** Activities of all users on the IFMIS system shall be monitored and audited on a regular basis.
- 2.1.4 Default Passwords:** All default passwords shall be changed upon implementation of the equipment on the IFMIS network.
- 2.1.5 IT responsibilities:** The IFMIS IT Administrators shall be responsible for the administration of access controls to all IFMIS computer systems.

- 2.1.6** Managing Passwords: The selection of passwords, their use and management as a primary means to control access to systems shall strictly adhere to the password. In particular, passwords shall not be shared with any other person for any reason.
- 2.1.7** Password Aging and Expiration: IFMIS system and user passwords shall be configured to expire after period of one month interval and thus forcing users to change their passwords. The password age is variable depending on outstanding circumstances on which the user is created.
- 2.1.8** Password History: The system shall be configured in such away that passwords already used on the IFMIS system are not re-used.
- 2.1.9** Password Complexity: IFMIS Passwords shall be a combination of both alpha/numeric characters and the minimum password length shall be set.
- 2.1.10** User responsibilities: IFMIS users shall be responsible for all computer transactions that are made with his/her User ID and password.
- 2.1.11** Automatic Locking: The Computers shall be configured in such away to automatically lock after 10 minutes of inactivity.
- 2.1.12** Users should log out of the computer when leaving a workstation for an extended period.
- 2.1.13** See Appendix ii for User Creation Approval

## **2.2 IFMIS NETWORK**

- 2.2.1** Configuring IFMIS Network: The IFMIS network shall be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.
- 2.2.2** Managing Network: Professionally qualified staff shall manage the IFMIS network, and preserve its integrity in collaboration with the nominated individual system owners.
- 2.2.3** Accessing IFMIS Network Remotely: remote access to the IFMIS network and resources shall only be permitted provided authorized users are authenticated, data is encrypted across the network, and privileges are restricted.
- 2.2.4** Defending IFMIS Network Information from Malicious Attack: IFMIS System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

## 2.3 SECURITY ADMINISTRATION

**2.3.1** IFMIS Security Policy will govern the security implementation on IFMIS resources.

**2.3.2** The implementation of the IT Security policy is the responsible of IFMIS management.

## 2.4 TESTING AND TRAINING

**2.4.1 Controlling IFMIS Test Environments:** Formal change control procedures shall be employed for all amendments to IFMIS system. All changes to programs must be properly authorized and tested in a test environment before moving to the IFMIS live environment.

**2.4.2 Using Live Data for Testing:** The use of IFMIS data for testing new system or system changes shall only be permitted where adequate controls for the security of the data are in place.

**2.4.3 Testing Software before transferring to a Live Environment:** Formal change control procedures shall be utilized for all amendments to the IFMIS systems. All changes to environment before moving to the live environment.

**2.4.4 Capacity Planning and Testing of New Systems:** New IFMIS systems shall be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience, which meets or exceed the technical and business needs and requirements of IFMIS.

**2.4.5 IFMIS Parallel Running:** Normal System Testing procedures shall incorporate a period of parallel run where necessary.

**2.4.6 Separation of development, test and operational facilities:** Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.

## 2.5 PHYSICAL SECURITY

**2.5.1 Securing Physical Protection of Computer Premises:** IFMIS computer premises shall be safeguarded against unlawful and unauthorized physical intrusion.

**2.5.2 Physical Access Control to secure Areas:** The IFMIS Data Centre shall be protected from unauthorized access using a biometric system as well as physical locks.

- 2.5.3 Managing On-Site Data:** Data capture shall be secured and IFMIS computers/terminals shall be secured.
- 2.5.4 Working in secure areas:** Physical protection and guidelines for working in secure areas shall be designed and applied by the Audit and Security Work Group.

## 2.6 EQUIPMENT SECURITY

- 2.6.1 Equipment Protection:** Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
- 2.6.2 Supporting utilities:** IFMIS equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
- 2.6.3 Equipment Maintenance:** Equipment shall be correctly maintained to ensure its continued availability and integrity.
- 2.6.4 Security of equipment off premises:** Security shall be applied to off-site equipment taking into account the different risks of working outside the IFMIS' sites.
- 2.6.5 Secure disposal/reuse of equipment:** All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely over-written and certified by the IT and Audit Security Work Groups prior to disposal.
- 2.6.6 Removal of property:** Equipment, information or software shall not be taken off site without prior authorization.

## 2.7 OPERATIONAL PROCEDURES AND CHANGE MANAGEMENT

- 2.7.1 Quality:** It is the policy of GOL and IFMIS that all equipment and software shall be at all times of high quality based on a Cost Benefit-Analysis.
- 2.7.2 Segregation of duties:** Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of IFMIS assets.
- 2.7.3 Maintenance:** All hardware equipment shall have maintenance as agreed in the SLA with the service provider.
- 2.7.4 Software:** All software shall be regularly upgraded as detailed in software SLA.

**2.7.5 Software Upgrade:** All major software will have to undergo the Change Management procedures.

**2.7.6 Documented operating procedures:** Operating procedures shall be documented, maintained, and made available to all users who need them.

**2.7.7 Change Management:** All system changes shall be controlled and approved by the IFMIS business owner.

**2.7.8** All changes shall follow detailed and agreed upon procedures.

**2.7.9** See Appendix iii for procedures on changes.

## 2.8 **INFORMATION SYSTEMS PROCUREMENT**

**2.8.1** To maintain consistent quality and adhere to IFMIS security standards and guidelines, all IFMIS additional hardware and software procurements shall be processed with the help of IT personnel according to agreed procurement procedures.

**2.8.2** Service Level Agreements for all IT related equipments shall be adhere to.

## 2.9 **VALIDITY AND REVIEW DATES**

**2.9.1** This shall remain valid until such a time that it is repealed by the Minister of Finance.

**2.9.2** The policy shall be reviewed from time to time but at a minimum of once a year.

## 2.10 **SECURITY INCIDENT MANAGEMENT**

All IFMIS users shall be responsible for reporting any suspected security Breaches or violations within 24 hours. Security incident management is broken down into three steps:

- i. Incident reporting
- ii. Incident recording
- iii. Incident response

### 2.10.1 INCIDENT REPORTING

It is important that information security incidents are reported quickly to ensure that action is taken to minimise the impact of the incident and prevent its recurrence.

IFMIS users who suspect a security breach or violation should communicate their concerns to the relevant authorities within 24 hours.

Security incidents shall be escalated to respective authorities in an efficient and timely manner.

**Types of Incidents:**

- i. Actual Incident
- ii. Potential/Likely Incident

The table below gives examples of the reportable incidents:

	Confidentiality	Integrity	Availability	Authenticity
Actual Incidents	Unauthorised access	Computer hacking	Unscheduled system loss	Deliberate dissemination of false information
	Theft or deliberate Leakage of information	Computer virus infection	Theft of equipment	Inability to identify a User
	Mis-direction of Sensitive mail	Suspicious hardware or software malfunctions	Sabotage or vandalism affecting IT services	Unauthorised modification of data
	Accidental broadcast Of sensitive mail	Fraudulent activities		
	Confidentiality	Integrity	Availability	Authenticity
Potential Incidents	Loss of diskettes, papers or laptops	Absence of Change control	Loss or failure to restore backup information from storage media such as disks, tapes, etc	Inability to identify the originator of the email

	<p>Logged on terminal or PC Left unattended</p>	<p>Operational use software not tested</p>	<p>Damage to fallback facility or service</p>	<p>Changes to data with no obvious reason or authorisation</p>
		<p>Failure to follow</p>	<p>Email chain</p>	
	<p>Identified security flaws in IT systems</p>	<p>Operational procedures</p>	<p>Letters</p>	
	<p>Discovery of unprotected documents or media</p>	<p>Virus detected on incoming diskette</p>	<p>Fire, flooding or power failures</p>	
	<p>Multiple reject attempts to access IT resources</p>			
	<p>Exposure of passwords</p>	<p>Use of unauthorised software (eg. Games)</p>	<p>Operation errors</p>	
	<p>Inadequate protection of classified information</p>		<p>Unusual application or operating system activity</p>	

### **2.10.2 INCIDENT RECORDING**

All reported incidents shall be captured and recorded using some agreed upon structured security reporting format. For any reported incident the following information should be included:

#### **Actual Incident**

- i. Date of incident
- ii. Time of incident
- iii. Place of incident
- iv. Name of reporter
- v. Incident Reference Indicator
- vi. Telephone/Extension
- vii. User email
- viii. Description of the incident
- ix. Action taken to limit the damage
- x. Review/comments by Head Section

#### **Potential / Likely Incident**

- i. Date of suspected incident
- ii. Time of suspected incident
- iii. Place of suspected incident
- iv. Name of reporter
- v. Incident Reference Indicator
- vi. Telephone/Extension
- vii. User email
- viii. Description of the incident
- ix. Action taken to limit the damage
- x. Review/comments by Head Section

### 2.10.3 Incident Response

The IFMIS Helpdesk shall handle all reported incidents and forward them to management for further investigation/resolution. Depending on the severity of the incident the following tasks shall be carried out:

- i. **Escalation:** If the incident is of high impact to IFMIS operations it is escalated to IFMIS management.
- ii. **Responsibilities** and procedures: Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
- iii. **Follow up:** measures shall be documented to improved effectiveness of response, identification of fault systems and management of the resources. Major incidents such as prolonged power outages should have a 'post event review' carried out.
- iv. **Disseminating learning:** knowledge from past incidents is passed on to staff to raise their awareness and appreciation of why their involvement in identifying information security incidents and system malfunctions is crucial for the continuity of MOF operations.
- v. **Incident Reporting procedures:** Information security events shall be reported through appropriate management channels as quickly as possible.

### 2.10.4 INFORMATION SECURITY INCIDENTS

- i. Responsibilities and procedures: Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
- ii. Learning from security Incidents: There shall be mechanisms in place to enable the types and volumes of information security to be documented into Lesson Learnt.
- iii. Collection of evidence: Evidence shall be collected, retained, and presented according to set procedures.

## 3.0 IFMIS ADMINISTRATION POLICIES

### 3.1 IFMIS SYSTEM ADMINISTRATION

**3.1.1 Managing IFMIS System Operations:** The IFMIS systems shall be operated and administered using documented procedures in a manner,

which is both efficient but also effective in protecting the system's information security. The service provider shall provide the system baseline documentation and High peak network performance documentation.

- 3.1.2 IFMIS System documentation:** The IFMIS System documentation shall be required and shall be kept up-to-date and be available whenever need arises.
- 3.1.3 Monitoring Error Logs:** Error logs shall be reviewed and managed by the assigned IT staff. Error Logs shall be reviewed on as a need basis depending on the criticality of the errors.
- 3.1.4 Error Logs:** Shall be kept for a period of at least 12 months.
- 3.1.5 Scheduling Changes to Routine Systems Operations:** Changes to routine IFMIS system operations shall be fully tested and approved before being implemented.
- 3.1.6 Approval of changes:** Authority shall be obtained from the Business Owner before changes are effected. See Appendix iii.

## 3.2 SECURING IFMIS DATA

- 3.2.1 Data Encryption:** Sensitive and confidential data shall always be transmitted in encrypted form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties and any possible issues from using encryption techniques.
- 3.2.2 Fire Risks to IFMIS systems:** All IFMIS data and information shall be protected against the risk of fire damage at all times. The level of protection must always reflect the risk of fire and the value and classification of the information as well as property being safeguarded.
- 3.2.3 Licensed Software:** To comply with legislation and to ensure software vendor support, the terms and conditions of all End User License Agreements shall be strictly adhered to on the IFMIS network systems.
- 3.2.4 Defending against Hackers, Stealth-and Techno-Vandalism:** Risks to the IFMIS systems and information shall be minimized by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices.
- 3.2.5 Applying 'Patches' to Software:** Patches to resolve software bugs shall only be applied where verified as necessary and with management authorization. They must be reputable source and shall be thoroughly tested before use on the IFMIS network systems.

- 3.2.6 **Upgrading IFMIS Software:** IFMIS software upgrades shall be properly tested before they are used in a live production environment.
- 3.2.7 **Defending against Virus Attack:** Without exception, Anti Virus Software shall be deployed across the IFMIS network with regular virus definition updates and scanning across servers, PCs and laptop computers.
- 3.2.8 **Installing Virus Scanning Software:** Anti virus software shall be chosen and installed on the IFMIS network systems from a proven leading supplier.
- 3.2.9 **Operating System Software Upgrades:** Upgrades to the Operating System of IFMIS computer systems must have the associated risks identified and be carefully planned, as well as incorporating testing fallback procedures.

### 3.3 ACCESS TO IFMIS INFORMATION AND SYSTEMS

- 3.3.1 **Managing Access Control Standards:** IFMIS Access control standards for information systems shall be established in a manner that carefully balances restrictions to prevent unauthorized access against the need to provide unhindered access in accordance with the needs of the GOL.
- 3.3.2 **Managing User Access:** Access to IFMIS systems shall be authorized by the system administrator, including the appropriate access rights (or privileges) and must be recorded in an Access Control List. The lists shall reflect the level of confidentiality, sensitivity and value of the data and be safeguarded accordingly.
- 3.3.3 **Managing Network Access Controls:** Access to the resources on the IFMIS network shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.
- 3.3.4 **Controlling Access to Operating System Software:** IFMIS Administrator access rights to operating system shall be restricted to those persons who are authorized to perform systems administration /management functions.
- 3.3.5 **Securing against Unauthorized Physical Access:** Physical access to high security areas (Data Centre/DRC) shall be controlled by effective identification and authentication techniques. Staff members with authorization to enter such areas are to be provided with information on the potential security risks involved. See appendix i.

**3.3.6** Controlling Remote User Access: IFMIS Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques.

### **3.4 SYSTEM LOGS & AUDIT TRAILS**

**3.4.1** All IFMIS information systems shall have facilities to monitor security breaches and failures. Specifically the following shall be important features:

**3.4.2 Audit Trails:** IFMIS management shall ensure that the system provides the Audit trails showing the following information:

- a. User Name
- b. User ID of the person effecting the change
- c. Information before change
- d. Information after change
- e. Time of logging in
- f. Time duration of login
- g. Terminal used to log in

**3.4.3 Protection of log information:** logging facilities and log information shall be protected against tampering and unauthorized access.

**3.4.4 Administrator and operator logs:** System administrator and system operator activities shall be logged.

**3.4.5 Fault Logging:** faults shall be logged, analyzed and appropriate action taken.

**3.4.6 Fault Logging Escalation:** All faults logged in the system shall be escalated to higher authority for immediate action.

**3.4.7 Security Event Logging:** All security related events shall be escalated to IFMIS Helpdesk for forward and action.

**3.4.8 Monitoring System Use:** Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly. i.e System usage and utilization shall be monitored on a daily basis by system administrators.

**3.4.9 Review:** All system logs shall be reviewed on a weekly basis, otherwise crucial ones shall be reviewed instantly as on a need basis.

### 3.5 LICENSES

- 3.5.1 It shall be IFMIS' policy for licenses to comply with all laws regarding intellectual property.
- 3.5.2 Non-compliance shall expose IFMIS and the responsible persons to civil and /or criminal penalties.
- 3.5.3 The IT personnel shall maintain records of software licenses in the software library and periodically scan computers to verify that only authorized software is installed.

### 3.6 SECURING HARDWARE, PERIPHERALS

**Objective:** To prevent unauthorized access to Hardware

- 3.6.1 **Managing and Maintaining Backup Power Generators:** Secondary and backup power generators shall be employed where necessary to ensure the continuity of IFMIS services during power outages.
- 3.6.2 **Installing and Maintaining Network Cabling:** IFMIS Network cabling shall be installed and maintained by qualify personnel to ensure the integrity of both the cabling and the wall-mounted sockets. Any unused network wall socket should be sealed-off and their status formally noted.
- 3.6.3 **Maintaining a Hardware Inventory or Register:** IFMIS formal Hardware Inventory of all equipment must be maintained and kept up to date at all times.

### 3.7 NETWORK ACCESS CONTROL

**Objective:** To prevent unauthorized access to networked services

- 3.7.1 **Policy on use of network services:** Users shall only be provided with access to services that they have been specifically authorized to use.
- 3.7.2 **User authentication for external connections:** Appropriate authentication methods shall be used to control access by remote users.
- 3.7.3 **Equipment Identification in networks:** Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
- 3.7.4 **Remote diagnostic and configuration port protection:** Physical and logical access to diagnostic and configuration ports shall be controlled.

- 3.7.5 Segregation in networks:** Groups of information services, users, and information systems shall be segregated on networks.
- 3.7.6 Network connection control:** The capability of users to connect to the network shall be restricted, inline with the access control policy and requirements of the IFMIS business applications.
- 3.7.7 Network routing control:** Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access policy of the IFMIS business applications.

### **3.8 NETWORK SECURITY MANAGEMENT**

**Objective:** To ensure protection of information on IFMIS network and the protection of the supporting infrastructure.

- 3.8.1 Network Controls:** IFMIS network shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
- 3.8.2 Security of Network services:** Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or out-sourced.
- 3.8.3 Routers and Switches:** All routers and switches connected to IFMIS production networks shall be monitored and audited.
- 3.8.4 Passwords for Routers and switches:** Passwords for Routers and switches on the IFMIS network shall be changed regularly in accordance with the IFMIS Password policy.
- 3.8.5 Configurations:** Routers and switches configurations shall comply with ISO standards and policies compliant to deployed protocols.
- 3.8.6 Memory of network devices:** memory on the routers and other network devices shall be upgraded when need arises.

### **3.9 SERVER SECURITY POLICY**

- i. This policy applies to all server equipment owned and /or operated by IFMIS.
- ii. All security-related events on critical or sensitive systems must be logged and audit trails monitored.
- iii. Security-related events shall be reported to IT security personnel, who will review logs and report incidents to management.

- iv. Audits shall be performed on a regular basis by authorized team within the GOL Audit team.
- v. Operating System configuration should be in accordance with approved operating guidelines.

### **3.10 VIRUS PREVENTION AND DETECTION**

**3.10.1** The IFMIS Security Administrator shall periodically communicate and sensitise all Users on the network about the hazards of viruses. The sensitisation shall include the potential damage that can be caused to both their personal information and also the impact on the rest of the IFMIS operations.

**3.10.2** The IFMIS Security Administrator shall maintain up-to-date anti-virus software on all systems on the IFMIS network at any given time.

**3.10.3** The guidelines below shall be strictly followed to reduce on the incidents of information/data loss and/or corruption due to virus infection:

- i. A file arriving by email from an unknown source should not be opened unless the accompanying email message identifies the sender as a known contact.
- ii. Users shall not install programs from any source and this includes freeware, shareware and any software which has not been vetted and cleared by the Security Administrator.
- iii. If users have to use any media to transfer documents from workstation to workstation they must be scanned with anti-virus software.
- iv. All virus incidents and cases of virus detection must be promptly reported to the IFMIS technical helpdesk.

### **3.11 IFMIS SYSTEMS AUDIT**

**Objective:** To maximize the effectiveness of and to minimize interference to/from the information systems audit.

**3.11.1 Information systems audit:** Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to IFMIS business processes.

**3.11.2 Protection of Information systems audit tools:** Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

### **3.12 FRAUD AND CYBER CRIME POLICY**

**3.12.1** Fraud and cyber Crime will be guided by the IFMIS ICT Policy

**3.12.2** Fraud control policy and awareness program shall be carried out on regular basis to all users.

**3.12.3** Any form of fraud detected shall be reported to management and investigation procedures will follow.

## **4.0 BUSINESS CONTINUTITY PLANNING**

**Objective:** To counteract interruptions to IFMIS business activities and to protect critical business processes from the effects of major failures of information systems and disasters and ensure their timely resumption.

### **4.1 IFMIS BACKUP, RECOVERY AND ARCHIVING**

**Objective:** To maintain the integrity and availability of information processing facilities.

**4.1.1 Restarting or Recovering System:** IFMIS management shall ensure that adequate back up and system recovery procedures are in place.

**4.1.2 Backing up Data:** IFMIS information and data stored shall be backed up regularly.

**4.1.3 Full Backups:** shall be done at the initial setup of the production environment and incremental Backups shall be done on regularly basis. Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed back-up policy.

**4.1.4 Managing Backup and Recovery Procedures:** Backup of the IFMIS data files and the ability to recover such data is a top priority. Management members are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the IFMIS business.

**4.1.5 Recovery and Restoring of Data Files:** Management shall ensure that the integrity of IFMIS data files during the recovery and restoration of the files is maintained.

**4.1.6 Fallover:** Redundancy shall be put in place in all critical single point of failures. Fallover will be configured on communication links as well as Application servers to ensure high availability.

## 4.2 DISASTER RECOVERY Center (DRC)

**Objective:** To ensure IFMIS system availability at all times.

**4.2.1 DRC:** A disaster recovery off site similar in terms of equipment and technology to the Data Center shall be set up in a distance of at least 20 miles away from the main Data Center. However in a short time, the DRC shall be located in Monrovia

**4.2.2 Information security in business continuity:** A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the IFMIS' business continuity.

**4.2.3 Business Continuity:** Events that can cause interruptions to IFMIS business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

**4.2.4 Developing and implementing BCP:** Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of critical IFMIS business processes.

**4.2.5 Business Continuity Plan (BCP):** A single framework of business continuity plans shall be maintained to ensure all plans are consistent in addressing information security requirements, and to identify priorities for testing and maintenance.

4. **Testing and maintaining BCP:** BCP shall be tested and updated regularly to ensure that they are up to date and effective.

## 4.3 IFMIS INTERCONNECTION POLICIES

**4.3.1** The IFMIS systems to be accessed by the users on other networks shall be identified by the GOL.

**4.3.2** The IFMIS management on behalf of GOL shall only permit required protocols and data to be accessed on other networks.

**4.3.3** Network Address Translation – NAT shall be implemented by GOL between the IFMIS and other interconnecting networks.

- 4.3.4 Both IFMIS and other inter-connected networks shall deploy strict anti-virus procedures to avoid one network infecting the other.
- 4.3.5 All users on both networks shall be required to use unique User-IDs and passwords to access the network resources and shall be given limited access privileges.
- 4.3.6 Both IFMIS and other inter-connected networks shall deploy strict administrative security management measures to ensure safety of both networks.
- 4.3.7 In the event that other inter-connected networks cause a security breach or loss to IFMIS, the other networks shall be responsible for the damage caused and vice-versa.
- 4.3.8 Internet connection to the IFMIS shall be through high capacity well configured firewalls.
- 4.3.9 All connections between IFMIS and other inter-connected networks shall be through well configured firewalls.

#### **4.4 RISK ASSESSMENT**

- 4.4.1 Refer to the IFMIS Risk Assessment manual.
- 4.4.2 **Risk assessments:** shall be conducted on any entity within IFMIS or any outside entity that has signed a Third Party Agreement with IFMIS
- 4.4.3 Risk assessments shall be conducted on any information system, to include applications, servers, and networks and any process or procedure by which these systems are administered and/or maintained.
  - 4. Periodic risk assessment exercises and determination of countermeasures on the IFMIS system shall be carried out.

## **5.0 ELECTRONIC FUNDS TRANSFER (EFT)**

### **13.1 NON DISCLOSURE OF INFORMATION**

- 5.1.1 Supplier/Employee account information shall not be disclosed to unauthorized persons.
- 5.1.2 Personal information shall be shared with Suppliers/Employees if that information is required to provide the product or service requested:

- i. Where it is necessary for completing the electronic transfers;
- ii. In response to any administrative order or other legal process which we believe requires IFMIS compliance;
- iii. To any IFMIS personnel conducting a legitimate credit/debt inquiry to verify the existence or condition of an account for a third party such as the Police, CID and Attorney General.
- iv. Suppliers/Employees will agree that IFMIS management will not be responsible for the release of any information to anyone not authorized by the information owner who obtain identify characteristics such as Supplier ID or Employee ID.

## **13.2 RIGHT TO FEEDBACK**

**5.2.1** Electronic Funds Transfer transactions shall be reflected on the monthly account statements in accordance with terms of the transactions.

## **5.3 BUSINESS DAY**

**5.3.1** The business days are Monday through Friday, excluding Holidays.

## **5.4 RIGHT TO STOP PAYMENT**

**5.4.1** In case of error or fraud, the payment shall be stopped in accordance with the law.

## **5.5 ERROR RESOLUTION NOTICE**

**5.5.1** The IFMIS Database/System administrators shall resolve any errors whenever possible, through the Help Desk System.

## **5.6 POLICY ON PGP KEYS (Pretty Good Privacy)**

**5.6.1** Both CBL and MOF shall generate new public keys every 3 months and expire previously used keys.

**5.6.2** Previously used keys cannot be re-used.

**5.6.3** Both CBL and MOF shall exchange these keys through the use of SFTP link that has available been established.

**5.6.4** Both Parties will verify that they have received the keys through email.

- 5.6.5** The exchanged public keys shall be signed using the private keys of both parties so as to enable file verification upon decryption.
- 5.6.6** Both CBL and MOF shall name persons who will be responsible for the key generation, key signing and keys verification. It is these named persons that will be given the necessary rights to generate, sign and verify the keys.
- 5.6.7** In case of a security breach e.g. leakage of a private or public key, the keys shall be immediately terminated and a new key generated.
- 5.6.8** All audit trails for key generation and other PGP activities shall be recorded and maintained.

## **5.7 POLICY ON SFTP KEYS**

- 5.7.1** SFTP Keys that have been created to enable terminal authentication shall be maintained permanently unless there is a need to be changed.
- 5.7.2** Both Access and Incident SFTP logs shall be recorded and maintained.

# APPENDIX I

## DATA CENTER /DRC VISISTORS' PASS

1. Name of visitor: \_\_\_\_\_

2. Date of visit: \_\_\_\_\_

3. Time in: \_\_\_\_\_

4. Time out: \_\_\_\_\_

5. Purpose of Visit: \_\_\_\_\_

6. Visited DC Personnel: \_\_\_\_\_

Authorized by DCM: \_\_\_\_\_

Signature: \_\_\_\_\_

**NOTE: I \_\_\_\_\_ (Name & signature of visitor)  
agree to abide by the**

**rules and procedures of the operations of the Data Center.**

**APPENDIX II**

**The Republic of Liberia**

**IFMIS COMPUTER USER FORM**

*(Paragraph 14 of the manual procedures to the IFMIS system)*

Our  
Ref.....  
Ministry/Agency/Local  
Govt.....  
Date.....

To: THE DME

Please update our IFMIS user profile, as set out below.

Name of employee
User name
Job description
Position
Responsibilities assigned to user
Remarks
Action required (include effective date when action is to be taken)

Signed.....

**Head of Department**

Signed.....

**Comptroller**

## APPENDIX III

### CHANGE REQUEST FORM

<b>Change Requestor</b>		<b>Date</b>		<b>Version</b>
<b>MOF Contact</b>				
<b>Change ref number</b>				

<b>Scope of Change</b>	
------------------------	--

<b>Detail Description of Change</b>	
-------------------------------------	--

<b>Assigned to</b>	
<b>Other parties to be involved</b>	

Timeline							
	Change Preparation				Change implementation	Acceptance/	
Change Phases	Scope / Task Description	Resources/Planning	Contingency Plan	Acceptance Criteria	Delivery	Acceptance	
Owner (HP)							
Date							
Owner MOF							

Date							

Downtime Window	
-----------------	--

Goals & Objectives – Scope of Change

Resources – Planning

Contingency Plan

--

Tests Definition – Acceptance Criteria

--

Detailed Description of the tasks to be implemented

Owner	Tasks Description	Estimated Time

**Approval – Sign-off**

<b>Organization</b>	<b>Name &amp; Surname</b>	<b>Approved / Reject</b>	<b>Date</b>	<b>Signature</b>
Data Center				

## **APPENDIX IV**

### **EQUIPMENT MOVEMENT AUTHORIZATION**

Name of Person Requesting to move equipments: \_\_\_\_\_

Date: \_\_\_\_\_

Reasons for Move: \_\_\_\_\_

Move From: \_\_\_\_\_

Temporarily or Permanent Move: \_\_\_\_\_

Authorizing Officer: \_\_\_\_\_

Signature: \_\_\_\_\_

---

**DATA CENTER MANAGER**