THE REPUBLIC OF LIBERIA

Ministry of Gender, Children and Social Protection

(MGCSP)

Comprehensive ICT Policy

MARCH 2020

Approval

_____ _____

Hon. Williametta Piso Saydee-Tarr
Minister

Date

Table of Contents

1. INTRODUCTION

1.1. OVERVIEW

The Ministry of Gender Children and Social Protection (MGCSP) is committed to the correct and proper use of its Information Technology (I.T.) resources in carrying out its mandate in accordance with the Act created by the National Legislature, Republic of Liberia, authorizing it to manage, direct and coordinate the Women, Girls, Children, and Social Protections affairs of the Country.

The inappropriate use of information technology (I.T.) resources could expose the MGCSP to risks including virus and malicious software attacks, theft and unauthorized disclosure of information, disruption of network systems and services or litigation. The purpose of these policies are to provide MGCSP employees and other users of its I.T. resources with clear guidance on the appropriate, safe and legal ways in which they can make use of the organization's I.T. resources.

These policies are mandatory and by accessing any I.T. resources, which are owned or leased by the MGCSP, users are agreeing to abide by the terms of these policies.

1.2. SCOPE

The policy applies to:

1. All Information Technology (I.T.) resources provided by the MGCSP;
2. All users (including MGCSP employee, contractors, sub-contractors, partners working at the MGCSP and authorized third party) utilizing any of the MGCSP I.T resources;
3. All users (both personal & MGCSP business related) of the MGCSP's Information Technology (I.T.) resources;
4. All connections to (locally, remotely, wired or wirelessly) the MGCSP network Domains (LAN/WAN/FIBER);
5. All connections made to external networks through the MGCSP network.

1.3. RESPONSIBILITY

The ICT Division is responsible for:

1. The provision of reliable computer systems which deploy appropriate technical safeguards against threats to their availability, operation, stability, and performance;
2. The management and security of the MGCSP network(LAN/WAN/FIBER)
3. The provision of facilities for information backups on MGCSP network file servers and other centralized information stores but excluding backups of the hard disks on individual computers;
4. The provision and management of anti-virus/spyware software throughout the MGCSP.
5. The provision of additional security measures to enable use of computer systems outside the normal working environment when this is appropriate and necessary;
6. The procurement of all IT networking equipment, software and services;
7. The installation of all software;
8. The installation of all IT equipment, including connection to the MGCSP network;
9. The provision of training, advice and guidance to computer systems users.

Each user of the MGCSP's I.T. resources is responsible for:

1. Complying with the terms of this policy and all other relevant MGCSP policies, procedures, regulations and applicable legislation;
2. Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;
3. Ensuring they only use user access accounts and passwords which have been assigned to them;
4. Ensuring all passwords assigned to them are kept confidential at all times and not shared with others;
5. Complying with instructions issued by designated information owners, system administrators, network administrators and/or the ICT Directorate on behalf of the MGCSP;
6. Reporting all lost, stolen or damaged I.T. devices to their immediate supervisors and the ICT Division;
7. Reporting all actual or suspected information security breaches immediately to their immediate supervisors or/and the ICTDivision
8. Reporting all misuse and breaches of this policy to their immediate supervisor;
9. Ensuring they return to their immediate supervisor; all MGCSP computer devices (e.g. laptop, smart devices, printer, mobile phone devices, removable storage devices,etc), information, important email messages and other important items (e.g. swipe cards, keys and I.D. badges,etc) before they leave the employment of the MGCSP or transfer to another Governmental agency.
10. Ensuring they remove or delete all non-MGCSP personal information and email messages (i.e. information which is of a personal nature and belongs to the user and not the MGCSP) from their MGCSP computer before they leave the employment

of the MGCSP, as it may not be possible to get a copy of this data from the MGCSP once the user has left the MGCSP.

1.4. ENFORCEMENT

1. The Ministry of Gender Children and Social Protection (MGCSP) reserves the right to take such action, as it deems appropriate against individuals who breach the conditions of these policies.
2. MGCSP employees, contractors, sub-contractors or partners' employee working for the Ministry who breach these policiesmay be subject to disciplinary action, including suspension and dismissal as provided for in the MGCSP**disciplinary procedure**.
3. Breaches of these policies by a third party commercial service providermay lead to the withdrawal of MGCSP information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between the MGCSP and the third party commercial service provider.

2. ACCEPTABLE USE POLICY

The MGCSP's Information Technology (I.T.) resources must not be used:

1. For excessive personal use;
2. For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
3. For political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
4. To knowingly misrepresent the MGCSP;
5. To enter into contractual agreements inappropriately (i.e. without authorization or where another form of agreement is required);
6. To create, view, download, host or transmit material (other than users who are authorized by the MGCSP to access such material for research etc.) of a pornographic or sexual nature or which may generally be considered offensive or obscene and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. O'Material is defined as information (irrespective of format), images, video clips, audio recordings, etc…
7. To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others;
8. To retrieve, create, host or transmit material which is defamatory;
9. For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
10. For any activity that would compromise the privacy of others;
11. For any activity that would intentionally cause disruption to the computer systems or networks belonging to the MGCSP or others;

12. For any activity that would deliberately cause the corruption or destruction of data belonging to the MGCSP or others;
13. For any activity that would intentionally waste the MGCSP's resources (e.g. employee time and Information Technology (I.T.) resources);
14. For any activity that would intentionally compromise the security of the MGCSP's Information Technology (I.T.) resources, including the confidentiality and integrity of information and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
15. For the installation and use of software or hardware tools which could be used to probe or break the MGCSP I.T. security controls;
16. For the installation and use of software or hardware tools which could be used for the unauthorized monitoring of electronic communications within the MGCSP or elsewhere;
17. To gain access to information systems or information belonging to the MGCSP or others which you are not authorized to use;
18. For creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements;
19. For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

The above list should not be seen as exhaustive, as other examples of unacceptable use of the MGCSP's I.T. resources may exist. The MGCSP has the final decision on deciding what constitutes excessive personal use.

3. MOBILE DEVICE POLICY

1. All mobile devices that access the MGCSP's Intranet and/or network must be compliant with MGCSP Information Security Policies and Standards.
2. Devices must use the following Operating Systems: Android 2.2 or later, IOS 4.x or later, and Windows Phone OS 7.1 or later.
3. Devices must store all user-saved passwords in an encrypted password store.
4. Devices must be configured with a secure password that complies with the MGCSP's password policy.
5. This password must not be the same as any other credentials used within the MGCSP.
6. Devices must not be altered or have any software/firmware installed, which is designed to gain access to functionality not intended to be exposed to the user.
7. Devices must be kept up to date with the manufacturer or network provided patches. At a minimum, patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with MGCSP anti-virus policy.
9. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal MGCSP network.

4. EMAIL POLICY

1. All messages distributed via the MGCSP email system, even personal emails, are MGCSP property. You must have no expectation of privacy in anything that you create, store, send or receive on the MGCSP's email system
2. Your emails can be monitored without prior notification if the MGCSP deems this necessary
3. Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature, email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:
4. An email message may go to persons other than the intended recipient. If it contains confidential or sensitive information, this could be damaging to the MGCSP.
5. Letters, files and other documents attached to emails may belong to others. By forwarding this information, without permission from the sender, to another recipient you may be liable for copyright infringement.
6. Email is a fast form of communication. Often messages are written and sent simultaneously, without the opportunity to check for accuracy. If you send emails with any libellous, defamatory, offensive, racist or obscene remarks, you and the MGCSP can be held liable.
7. An email message may legally bind the MGCSP contractually in certain instances without the proper authority being obtained internally.
8. Email messages can carry computer viruses. If you send an attachment that contains a virus, you and the MGCSP can be held liable. By opening emails and attachments from an unknown sender you may introduce a virus into the MGCSP computing environment.

Rule of Email Use

The MGCSP considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image. Users should take the same care in drafting an email as they would for any other communication. Therefore, the MGCSP wishes users to adhere to the rules below:

1. The MGCSP name is included in the heading carried with every message sent by a MGCSP authorized user. Emails reflect on the Ministry image and reputation. Therefore, email messages must be appropriate and professional.
2. It is strictly forbidden to use MGCSP email system for anything other than legitimate business purposes. Therefore, the sending of personal emails, chain letters, junk mail, and jokes is prohibited. All messages distributed via the MGCSP's email system are the MGCSP property.
3. All emails will carry a disclaimer stating that the email is intended only for the MGCSP use and if used for any other purpose, a named person should be contacted immediately within the MGCSP.

4. Particular care should be taken when sending confidential or commercially sensitive information. If in doubt, please consult your superior.
5. MGCSP confidential messages should be distributed to authorized personnel only. Forwarding to locations outside is prohibited.
6. Great care must be taken when attaching documents or files to an email. Letters, files and other documents attached to emails may belong to others.
7. By forwarding this information, without permission from the sender, to another recipient you may be liable for copyright infringement. Again, if in doubt, please consult your superiors.
8. Subscription to electronic services or other contracts on behalf of the MGCSP is prohibited unless you have the express authority from an authorized member of senior management to do so.
9. If you receive any offensive, unpleasant, harassing or intimidating messages via email or intranet you are requested to inform your Manager or the IT Division immediately. It is important that we trace such emails as quickly as possible.

Inappropriate Use

All MGCSP Accounts are subject to the MGCSP's Acceptable UsePolicy. In addition, with respect to MGCSP's Email Accounts, any inappropriate email usage, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such email should immediately contact the ICT Division.

The exchange of email content that:

1. Generates or facilitates unsolicited bulk commercial email;
2. Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
3. Violates, or encourages the violation of, the legal rights of others;
4. Is for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
5. Intentionally distributes viruses, worms, trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
6. Alters, disables, interferes with, or circumvents any aspect of the email services;
7. Tests or reverse-engineers the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
8. Constitutes, fosters, or promotes pornography;
9. Is excessively violent, incites violence, threatens violence, or contains harassing content;
10. Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
11. Improperly exposes trade secrets or other confidential or proprietary information of another person;
12. Misrepresents the identity of the sender of an email.

13. Is otherwise malicious, fraudulent or may result in retaliation against the University by offended viewers.

Other improper uses of the email system include:

1. Collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting);
2. Use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
3. Any conduct that is likely to result in retaliation against the MGCSP's network or website, or the MGCSP's employees.
4. These guidelines provide some examples of permitted or prohibited use of email. This list is not intended to be exhaustive but rather to provide some illustrative examples.

5. MONITORING POLICY

1. The MGCSP shall implement procedures to monitor among others, access to systems and applications, fault logging, and the overall functional health of systems, networks and applications.
2. Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
3. Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
4. Logging facilities and log information shall be protected against tampering and unauthorized access.
5. System administrator and system operator activities shall be logged.
6. Faults shall be logged, analysed, and appropriate action taken.
7. The clocks of all relevant information processing systems within the MGCSP or domain shall be synchronized with an agreed accurate time source.

6. REGULATORY COMPLIANCE POLICY

1. The MGCSP shall identify relevant regulatory frameworks and clearly establish compliance with such frameworks.
2. Procedures shall be established for compliance with the MGCSP's own policies and procedures.
3. An independent system audit shall be carried out on all critical infrastructures at least once a year.
4. All relevant statutory, regulatory and contractual requirements and the MGCSP's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the MGCSP.

5. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
6. Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
7. Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
8. Users shall be deterred from using information processing facilities for unauthorized purposes.
9. Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
10. Information systems shall be regularly checked for compliance with security implementation standards.

7. DATA CLASSIFICATION POLICY

1. The data classification system has been designed to support the need to know so that information will be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, the MGCSP unduly risks loss of public confidence, internal operational disruption, and excessive costs.
2. All data at the MGCSP shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component with the aggregated information.
3. Restricted/Confidential: Data in any format collected, developed, maintained or managed by or on behalf of the MGCSP, or within the scope of the MGCSP activities that are subject to specific protections under the laws of Liberia or under applicable contracts. The unauthorized or accidental disclosure of this restricted information could adversely impact the MGCSP, its employees and operational mandate.
4. Sensitive: Data whose loss or unauthorized disclosure would impair the functions of the MGCSP, cause significant financial or reputational loss or lead to likely legal liability.
5. Public: Information that is available to the general public and intended for distribution outside the MGCSP. This information may be freely disseminated without potential harm. Data that does not fall into any of the other information classifications may be classified as public. This data may be made generally available without specific information owner's designee or delegate approval.
6. Internal Use Only: Confidentiality of data is preferred, but information contained or mark internal use only may be subject to open records disclosure. Internal Use Only information are to be disclosure to authorize person only.

8. ENCRYPTION POLICY

1. The use of encryption to protect a data asset will be the result of a data classification decision made by the asset's data owners. The requirement to use or not use encryption will be based on the classification level assigned to a data asset. The classification level assigned to a data asset will be based on the MGCSP's Data Classification Policy.
2. Cryptographic private or shared keys, cryptographic secrets, or authentication secrets or hashes will be classified at the highest classification level as outlined by the MGCSP's Data Classification Policy and protected using controls defined at that classification level.
3. The MGCSP will maintain documented procedures for supported cryptographic algorithms, by data classification level, which include documentation of:
    1. Acceptable cryptographic key lengths
    2. Acceptable cryptographic algorithms

4. The organization will maintain documented procedures for cryptographic key management which include documentation on the processes of:
    1. Generating cryptographic keys
    2. Distributing cryptographic keys
    3. Escrowing cryptographic keys
    4. Enabling authorized users to access stored cryptographic keys
    5. Changing and updating cryptographic keys
    6. Revoking cryptographic keys
    7. Archiving cryptographic keys
    8. Auditing and logging cryptographic key management

9. PERSONAL USE POLICY

The MGCSP's Information Technology (I.T.) resources are to be used primarily for MGCSP business-related purposes. However at the discretion of their immediate supervisors, occasional personal use may be permitted by a user provided it:

1. Is not excessive;
2. Does not take priority over their MGCSP work responsibilities;
3. It does not interfere with the performance and work of the user, other employee or the MGCSP;
4. Does not incur unwarranted expense or liability for the MGCSP;
5. Does not have a negative impact on the MGCSP in any way;
6. Does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
7. Is lawful and complies with this policy and all other relevant MGCSP policies
8. The MGCSP has the final decision on deciding what constitutes excessive personal use.
9. The MGCSP does not accept liability for any fraud or theft that results from a user's personal use of the MGCSP's Information Technology (I.T.) resources.

10. DATA RETENTION & DESTRUCTION POLICY

The MGCSP's staff and outsiders (independent contractors via agreements with them) are required to honor the following rules:

1. Paper or electronic documents indicated under the terms for retention in the following section will be transferred and maintained by management;
2. All other paper documents will be destroyed after **three years**;
3. All other electronic documents will be deleted from all individual computers, databases, networks, and back-up storage after **one year**;
4. No paper or electronic documents will be destroyed or deleted if pertinent to any on-going or anticipated government investigation or proceeding or private litigation and;
5. No paper or electronic documents will be destroyed or deleted as required to comply with government auditing standards.

Record Retention

The following table indicates the minimum requirements and is provided as guidance to customize in determining the MGCSP's document retention policy.

Type of Document	Minimum Requirement
Accounts payable ledgers and schedules	7 years
Audit reports	Permanently
Bank reconciliations	2 years
Bank statements	3 years
Checks (for important payments and purchases)	Permanently
Contracts, mortgages, notes, and leases (expired)	7 years
Contracts (still in effect)	Contract period
Correspondence (general)	2 years
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2 years
Deeds, mortgages, and bills of sale	Permanently
Depreciation schedules	Permanently
Duplicate deposit slips	2 years
Employment applications	3 years
Expense analyses/expense distribution schedules	7 years
Year-end financial statements	Permanently
Insurance records, current accident reports, claims, policies, and so on (active and expired)	Permanently
Internal audit reports	3 years
Inventory records for products, materials, and supplies	3 years
Invoices (to customers, from vendors)	7 years
Minute books, bylaws, and charter	Permanently
Patents and related papers	Permanently

Type of Document	Minimum Requirement
Payroll records and summaries	7 years
Personnel files (terminated employees)	7 years
Retirement and pension records	Permanently
Tax returns and worksheets	Permanently
Timesheets	7 years
Trademark registrations and copyrights	Permanently
Withholding tax statements	7 years

11. INFORMATION SYSTEMS DEVELOPMENT POLICY

1. Security requirements shall be defined and documented prior to the acquisition and development of a system or application.
2. The MGCSP shall establish a formal procedure for the development of its systems with a security component at all stages of the development.
3. In other to prevent unauthorized modification of information, errors, and the misuse of information, controls shall be established to validate input, output, and also to ensure message integrity.
4. System files shall be protected from unauthorized modification and tampering.
5. Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
6. Data input to applications shall be validated to ensure that this data is correct and appropriate.
7. Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
8. Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
9. Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
10. There shall be procedures in place to control the installation of software on operational systems.
11. Test data shall be selected carefully, and protected and controlled.
12. Access to program source code shall be restricted.
13. The implementation of changes shall be controlled by the use of formal change control procedures.
14. When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on operations or security.
15. Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
16. Opportunities for information leakage shall be prevented.
17. Outsourced software development shall be supervised and monitored by the MGCSP.

12. IT DEVICE AND EQUIPMENT POLICY

1. The Procurement Division must purchase all MGCSP I.T. devices and equipment through recognized and certified vendor with technical specification from the ICT Division. All devices or equipment should be subject to one-year mandatory factory warranty.
2. The ICT Division must approve all MGCSP I.T. devices and equipment, which has not been purchased through recognized and certified vendor, before being allowed to connect to the MGCSP network.
3. All I.T. devices and equipment provided by the MGCSP and/or its partners remain the property of the MGCSP. Users must not remove or borrow MGCSP I.T. devices or equipment without the authorization of their Manager/Director.
4. The security of any MGCSP I.T. devices and equipment borrowed is the responsibility of the borrower and the borrower must return the I.T. devices and equipment before they leave the employment of the MGCSP or, at the request of the borrower's supervisor/director or the ICT Division.
5. Users must not alter the hardware or software configuration of any MGCSP I.T. device or equipment without the prior authorization of the ICT Division.
6. Users must take due care when using MGCSP I.T. devices and equipment and take reasonable steps to ensure that no damage is caused to the I.T. device or equipment. They must not use I.T. devices and equipment (either in a MGCSP facility, while traveling or at home) if they have reason to believe it is dangerous to themselves or others.
7. Users must report all damaged, lost or stolen MGCSP I.T. devices and equipment to their unit supervisor/director and the ICT Division.
8. The ICT Division on behalf of the MGCSP reserves the right to remove any I.T. devices and equipment from the network at any time, for reasons including but not limited to the following:
    1. Non-compliance with MGCSP policies,
    2. The I.T. device or equipment does not meet approved specification and standard, or
    3. The I.T. device or equipment is deemed to be interfering with the operation of the network.

13. INCIDENT RESPONSE POLICY

1. All Computer Security Incidents must be reported to the ICT Division.
2. Follow appropriate Incident Handling procedures as specified in the policy
3. In the event that a User detects a suspected or confirmed Computer Security Incident, the User must report it to the IT Division for issues including but not limited to viruses, worms, local attacks, denial of service attacks, or possible disclosure of Confidential MGCSP Data.
4. An Immediate Response Team (HELP DESK) must be established to supplement the MGCSP's information security infrastructure and minimize the threat of damage resulting from Computer Security Incidents.

5. The Immediate Response Team (HELP DESK) shall be created for Confidential Data Security Incidents.
6. Membership on the Immediate Response Team (HELP DESK) shall be as designated by the ICT Director with key members from IT Network Security included.
7. Responsibilities of the Immediate Response Team (HELP DESK) are to assess the incident and follow incident handling procedures, appropriate to the incident as determined by the IT Division.
8. Immediate Response Team (HELP DESK) members will share information about security incidents beyond the Immediate Response Team (HELP DESK) only on a need-to-know basis, and only after consultation with all other team members.

Incident Handling

For incidents requiring the formation of an Immediate Response Team (HELP DESK), the following is a list of response priorities that should be reviewed and followed as recommended by the ICT Director. The most important items are listed first:

1. Safety and Human Issues. If an information system involved in an incident that affects human life and safety, responding to any incident involving any life-critical or safety-related system is the most important priority.
2. Establish Scope of Incident. The Immediate Response Team (HELP DESK) shall promptly work to establish the scope of the incident and to identify the extent of systems and data affected. If it appears that personally identifiable information may have been compromised, the Immediate Response Team (HELP DESK) shall immediately inform the ICT Director.
3. Containment. Once life-critical and safety issues have been resolved, the Immediate Response Team (HELP DESK) shall identify and implement actions to be taken to reduce the potential for the spread of an incident or its consequences across additional systems and networks. Such steps may include requiring that the system be disconnected from the network.
4. Develop Plan for Preservation of Evidence. The Immediate Response Team (HELP DESK) shall develop a plan promptly upon learning about an incident for identifying and implementing appropriate steps to preserve evidence, consistent with needs to restore availability. Preservation plans may include preserving relevant logs and screen captures. The affected system may not be rebuilt until the Immediate Response Team (HELP DESK) determines that appropriate evidence has been preserved. Preservation will be addressed as quickly as possible to restore availability that is critical to maintain business operations.
5. Investigate the Incident. The Immediate Response Team (HELPDESK) shall investigate the causes of the incident and future preventative actions. During the investigation phase, members of the incident response team (HELP DESK) will attempt to determine exactly what happened during the incident, especially the vulnerability that made the incident

possible. In short, investigators will attempt to answer the following questions: Who? What? Where? When? How?

6. Incident-Specific Risk Mitigation. The Immediate Response Team (HELP DESK) shall identify and recommend strategies to mitigate risk of harm arising from the incident, including but not limited to reducing, segregating, or better protecting personal, proprietary, or mission critical data.
7. Restore Availability. Once the above steps have been taken, and upon authorization by the Immediate Response Team (HELP DESK), the availability of affected devices or networks may be restored.
8. MGCSP-Wide Learning. The Immediate Response Team (HELP DESK) shall develop and arrange for implementation of a communications plan to disseminate knowledge obtained from the security incident throughout the MGCSP to individuals in order to reduce the risk of recurrence of such incident.

Documentation

1. Log of security incidents. -Immediate Response Team (HELP DESK) shall maintain a log of all reportable security incidents recording the date, department affected, whether or not the affected machine was registered as a critical host, the type of Confidential MGCSP Data affected (if any), number of subjects (if applicable), and a summary of the reason for the intrusion, and the corrective measure taken must be recorded.
2. Critical Incident Report. -The Immediate Response Team (HELP DESK) shall issue a Critical Incident Report for every reportable security incident affecting machines qualifying as Critical Hosts, or other priority incidents, describing in detail the circumstances that led to the incident, and a plan to eliminate the risk.

Best Practice

Preserving Evidence: It is essential to consult the ICT Security Analyst when handling Computer Security Incidents. However, if the ICT Security Analyst is not available for emergency consultation, the following practices are recommended:

1. Generally, if it is necessary to copy computer data to preserve evidence for an incident, it is a good idea to use bit-wise file-system copy utilities that will produce an exact image, rather than to use file level utilities, which can alter some file meta-data.
2. When making forensic backups, always take a cryptographic hash (such as an SHA-1 hash) of both the original object and of the copied object to verify the authenticity of the copy.
3. Assigning members to an Immediate Response Team (HELP DESK): In cases where an incident involves an investigation into misconduct, the MGCSP should consider carefully whom to assign to the Immediate Response Team (HELP DESK). For example, one may not wish to assign

an IT professional who works closely with the individual(s) being investigated.

14. OUTSOURCING POLICY

1. MGCSP continuously explores, and where appropriate, implements organizational changes that improve efficiency and effectiveness, in the service of its mandated goals and objectives. MGCSP will consider outsourcing of services or functions currently performed by MGCSP staff or partner where such outsourcing could improve efficiency and effectiveness and allow MGCSP to dedicate itself to its core mission.
2. MGCSP will approach outsourcing with care and due diligence. Proposals to outsource will include a rigorous cost benefit analysis that takes into account both economic factors and potential impacts on affected staff and MGCSP. MGCSP will approve proposals to outsource only where the proposal is supported by a clear and achievable business case.
3. A decision to outsource has implications for the entire MGCSP, including relations with the staff associations and external constituencies. For this reason, final decisions relating to outsourcing will be made at the Minister's level.
4. When considering a proposal for outsourcing, MGCSP will ensure that:
    a) Effective, appropriate consultation should occur with Division/Unit within the MGCSP whose staff may participate in the outsourcing process.
    b) Proposals are developed and implemented in accordance with all MGCSP Policies and applicable agreements.
    c) Complete information on the business case for outsourcing, including detail of the advantages and disadvantages of all options considered, is provided to staff members participating in the outsourcing process.
    d) Any consideration to outsource is supported by a clear business case from which a business plan can be developed that details all aspects of implementation, which is reflected through a request for proposals process that the business case is achievable.
    e) A thorough evaluation process in accordance with the PPCC procurement acts of the Republic of Liberia is implemented to determine the success of the outsourcing should the proposal be approved.

15. WIRELESS POLICY

All wireless infrastructure devices that reside at a Ministry site and connect to a MGCSP network, or provide access to information classified as Confidential, or Restricted must:

1. Be installed, supported, and maintained by an approved support team.
2. Use MGCSP approved authentication protocols and infrastructure.
3. Use MGCSP approved encryption protocols.
4. Maintain a hardware address (MAC address) that can be registered and tracked.

5. Not interfere with wireless access deployments maintained by other support organizations.

16. DATA CONFIDENTIALITY POLICY

1. For authorized personnel, confidential data may be made available on a need to know basis as and when required. For all other persons, access to such information must be prohibited.
2. Unauthorized modification, transmitting or other dissemination of confidential information is strictly prohibited.
3. Unauthorized dissemination of this information may result in disciplinary or legal action as appropriate.
4. Confidential information should be safely stored and protected while on file servers, network drives, workstations, and during any type of transmission. Authorized access should be enforced.
5. Confidential information should be erased securely from network drives, file shares etc. after proper authorization.
6. Network or directory share information showing where the confidential information is stored must not be publicly viewable.
7. Confidential data must not be emailed or texted; unless there is no other method available to transmit the information.
8. Upon prior authorization, confidential information sent via email must be sent from their official work email account. Confidential information sent via email off-site must be encrypted.
9. Employees must not download and store confidential information unless encrypted on their personal computers, external hard drives, thumb/ pen drives and CD/DVD, or any removable device.
10. Printed reports that contain confidential data must not be left available to the public. All printed confidential data must be shredded or disposed of into locked bins.
11. Employees must not take printed or unencrypted confidential data off MGCSP premises.
12. Employees must not discuss confidential data in public.

17. BUSINESS CONTINUITY & DISASTER RECOVERY POLICY

1. A business continuity and disaster recovery management plan shall be established.
2. The plan shall be tested at least once a year of all critical applications and systems.
3. A managed process shall be developed and maintained for business continuity throughout the MGCSP that addresses the information security requirements needed for the MGCSP's business continuity.
4. Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

5. 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 business processes.
6. A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
7. Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

18. THIRD PARTY MANAGEMENT POLICY

1. The MGCSP shall establish procedures to manage agreements with third parties, including, but not limited to, access to information and monitoring of service level agreements.
2. The risks to the MGCSP's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
3. Security risks with third party contractors working onsite shall be identified and appropriate controls are implemented.
4. All identified security requirements shall be addressed before giving third parties access to the MGCSP's information assets.
5. Agreements with third parties involving accessing, processing, communicating or managing the MGCSP's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements to ensure compliance with the MGCSP's security policies and standards.
6. It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.
7. The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
8. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
9. Contracts with third parties to outsource the management and control of all or some of the MGCSP information systems, networks and/or desktop environments shall address security requirements.

19. RECORDS MANAGEMENT POLICY

1. MGCSP will meet legal record keeping requirements and will seek to comply with relevant codes of practice for all its records in all media and formats.
2. Information is available when needed;
3. Closed records are moved to inactive storage;
4. Records of permanent value are preserved in MGCSP's Archives; and

5. Non-permanent records are destroyed according to the retention schedule and to procedures for destroying confidential records.
6. Records are present - information necessary to document and reconstruct MGCSP's activity has been recorded
7. Records are accessible - records can be located and retrieved in a way which is true to the original presentation of the information
8. Records can be interpreted - context can be shown, establishing when, where and who created it, how it was used and how it is related to other records
9. Records can be trusted - the integrity and authenticity can be demonstrated beyond reasonable doubt
10. Records can be maintained - records are present, accessible, interpreted and trusted for as long as they are required, through transfer to other locations, systems or technologies.
11. MGCSP will preserve its records according to the retention periods in its Records retention schedule.
12. Appropriate storage conditions for paper records will be provided. Electronic records will be maintained during any changes in the infrastructure, so that they continue to fulfil policy requirements.
13. Records that have been identified as confidential by the Records retention schedule will continue to be restricted, as required. Decisions to allow access to confidential records will be made by the staff identified for this responsibility in the Records retention schedule.
14. When considering external access to its records, the MGCSP recognizes its responsibilities towards educational research and attempts to support this process, while complying with legal record keeping requirements and the reasonable expectation of confidentiality of its stakeholders.
15. Some records may be subject to legislation requiring them to be either withheld or made more widely available outside the MGCSP.

20. ASSET DISPOSAL POLICY

1. Reasonable effort will be made to see if any other team is able to make use of the equipment.
2. Where this is not possible, consideration must be given to determine if the equipment can be donated to a school, charitable organization or community project or auctioned to employees. It is necessary that someone (i.e. someone within MGCSP) who is interested in the particular good cause should volunteer to take charge of the process, and act as MGCSP agent in ensuring that proper steps are taken per this policy. MGCSP should incur no charges through this process.
3. If the equipment cannot be reused, then it will be recycled or disposed of as scrap via an authorized contractor.
4. The MGCSP policy for disposal of equipment that cannot be economically repaired is to recycle or dispose of it as scrap via an authorized contractor.
5. Before disposing of any computer system, it is vital to remove all traces of data files.

21. INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY

1. Copyright - The MGCSP shall ensure compliance with the legal restrictions on the use of material in respect of which there may be IPR, such as copyright, design rights and trademarks.
2. Only licensed Software will be used on MGCSP system, and must be procured through approved vendors and included in the MGCSP system asset list.
3. All licenses will be stored centrally under secure conditions and checked so that they may be kept up-to-date.
4. Regular checks on all parts of the system will be carried out to ensure that only licensed products are installed.
5. Disciplinary action will be taken against those who have breached such copyrights.
6. Safeguarding of MGCSP System Records – All MGCSP system records will be protected in accordance with the provisions of ISO 27001.
7. All MGCSP staff must be made aware of the requirement that they may only use the system and its applications for which they are authorised that are detailed on the user registration form.

22. THIRD PARTY CONNECTION POLICY

1. The ICT Division is responsible for all external connections to the MGCSP's network.
2. In general, direct connection to the MGCSP network from contracted third parties providing computing or network support will be allowed.
3. Contracted third parties with special connections must agree to abide by any and all computing-related policies, especially security and privacy policies, of the MGCSP.

4. Access to the MGCSP's network is a privilege that may be granted or withdrawn by the MGCSP at any time.
5. The MGCSP may terminate the special connection if it is determined not to be in the MGCSP's interest to continue the connection.
6. The MGCSP may also impose temporary service interruptions for operational reasons.

23. CLEAR DESK & SCREEN POLICY

1. In the interest of security and good practice, personnel are to ensure that they maintain a 'clear desk' policy.
2. This means that desks are to be kept as clear as possible at all times.
3. It is the MGCSP policy that all desks are to be cleared at the end of each day.
4. Additionally, personnel are to de-activate their screens if there is a possibility of eavesdropping by unauthorized persons.
5. Workstations or laptops must also be 'locked' immediately when left unattended for any length of time.

24. ENVIRONMENTAL CONTROL POLICY

1. The MGCSP shall formally conduct a risk assessment to determine environmental threats to its personnel, equipment, and systems.
2. The MGCSP shall establish and implement procedures for ensuring that equipment are protected from environmental threats identified in (1) above.
3. The power and telecommunications cable carrying data or supporting information services shall be protected from interception or damage.
4. Equipment shall be maintained as per the supplier's recommended service intervals and only authorized and certified personnel shall carry out specifications and the maintenance.

25. MEDIA HANDLING POLICY (REF: COMMUNICATION DIVISION)

1. Procedures shall be established for records management, handling media in transit, at rest, and media off-site.
2. There shall be procedures in place for the management of removable media.
3. Media shall be disposed of securely and safely when no longer required, using formal procedures.
4. Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
5. System documentation shall be protected against unauthorized access.

26. GUEST ACCESS POLICY

1. The MGCSP may frequently host guests or third parties who maybe providing a service, but are not official employees of the MFDP. Parties to this classification ARE permitted guest services.
2. The MGCSP may invite vendors as well as members of the news media, who are there at the behest of the MGCSP and/or providing a service to the MGCSP. Parties to this classification ARE permitted guest services.
3. The MGCSP may frequently hosts meetings and other gatherings for various purposes. Parties to this classification ARE permitted guest services as long as prior evaluation and approval is granted.
4. The MGCSP agrees to provide wireless network access to guests for purposes of casual web surfing and exchange of communications (such as e-mail or other messaging). All use is subject to various MGCSP policies including Acceptable Use Policy, which all guests must agree to before service is provided.
5. Guests will be provided with either a unique account or ID, or a group-unique registration account, for their exclusive use to register their wireless devices on the wireless network.
6. Wireless network access for guests is provided at a "best effort" level, and no expectations or assumptions should be made about the quality or availability of

service. Guests will not be provided any technical support by the IT Division, including assistance configuring their wireless device.

7. All guest access to the wireless network requires sponsorship by an entity within the MGCSP. They must fill out a guest access form that will get submitted to the ICT Division. Requests should be made at least 24 to 48 hours before access is desired.

26. APPENDIX

26.1 Incident Response Form (HELP DESK)

INCIDENT IDENTIFICATION INFORMATION	
Date and time of notification:	
Status:	
LEAD BY	**REPORTED BY**
Name:	Name:
Title:	Title:
Contact Information:	Contact Information:

INCIDENT SUMMARY			
Severity:		**Location:**	
Type of incident Detected: ☐Denial of Service ☐Malicious Logic	☐Unauthorised Access ☐Unauthorised Use	☐Unplanned Downtime ☐Other	
Description of Incident:			
Affected Systems:		**User Groups Affected:**	
Experienced Downtime:			
Host	**Dates/Times**	**Details**	**Affected Users**

INCIDENT NOTIFICATION		
☐IT Management	☐Application/System Owner	☐Affected Users
☐IT Risk Management Team	☐Human Resources	☐Legal and Risk
☐Service/System Administrator	☐Application/System Vendor	☐Law Enforcement
☐Other:		
Names and Contacts of Persons Involved		

ACTION SUMMARY
Identification Measures:
Containment Measures:
Evidence Collected:
Eradication Measures:
Back-out Strategy:
Other Mitigation Actions:

POST INCIDENT ANALYSIS

Incident Summary:

Cause of Incident:

Damage Caused:

Actions Pending Implementation:

Action	Status	Assignee	Team:	Expected Delivery Date	Date Raised	Date Completed

Lessons Learnt:

26.2 Incident Security Severity

- Incidents are categorized at one of three severity levels based on the impact to the Ministry of Gender Children and Social Protection (MGCSP) as a whole. The following table provides general definitions and description of each severity level:

SECURITY LEVEL	DEFINITION	EXAMPLES
HIGH	Incidents that have a severe impact on the organization's business or services	▪ Malicious code ▪ Unauthorised access ▪ DOS affecting critical services ▪ Compromise of host containing sensitive data
MEDIUM	Incidents that have significant impact on the organization's business or services	▪ Attempts to gain unauthorised access ▪ Open mail relay
LOW	Incidents that have minimal impact on the organization's business or services	▪ Unauthorized network probes or system scans ▪ Isolated virus infections

26.3 Policy Exemption Request Form

This form is to be completed and sent to the IT Director by those requesting an exemption from Information Security Policy.

Policy Exemption Required:

_____

_____

Requested by:

_____

Reason Exemption Required:

_____

_____

_____

_____

Department/ Personnel to whom the Exemption should apply: _____

_____

Period of Exemption From: _____To_____

Comments by ICT Director _____

_____

_____

_____

State whether exemption is Granted or Rejected: _____

Signed: _____ Dated: _____

26.4 Policy Acknowledgement Form

I acknowledge that I have received a copy of the Policy and Procedures Manual, which describes important information about the Ministry of Gender Children and Social Protection (MGCSP), and understand that I should consult the Human Resource Division (DMS) if I have questions.

I have entered into employment with the Ministry of Gender Children and Social Protection (MGCSP) voluntarily and acknowledge that it is for no specified length of time. Accordingly, either I or the Ministry of Gender Children and Social Protection (MGCSP) may terminate the relationship at will, with or without cause, at any time, for any reason or no reason.

I understand that neither this policy nor any other Ministry of Gender Children and Social Protection (MGCSP) policy, practice or procedure is intended to provide any contractual obligations related to continued employment, compensation or employment contract.

I understand that the Ministry of Gender Children and Social Protection (MGCSP) may change, modify, suspend, interpret or cancel, in whole or part, any of the published or unpublished personnel policies or practices, with or without notice, at its sole discretion, without giving cause or justification to any employee.

Such revised information may supersede, modify or eliminate existing policies. The Ministry of Gender Children and Social Protection (MGCSP) management shall have sole authority to add, delete or adopt revisions to the policies in this Manual. Any written or oral statement by a supervisor or department director contrary to the personnel policy manual is invalid and should not be relied upon by any employee.

I understand and agree that I will read and comply with the policies contained in this Manual and any revisions, am bound by the provisions contained therein, and that my continued employment is contingent on following those policies.

_____

Employee Name (Printed)

_____

Employee Signature

_____

Date

26.5 Guest Network Account Form

Guest Network Account Request Form

Name: _____Telephone Number: _____

E-mail Address: _____

Company Information

Company Name: _____
Telephone Number: _____
Address: _____
City: _____

DURATION OF VISIT - Please indicate the exact dates you are requesting access.
Beginning Date: _____ End Date: _____

Applicant's Signature _____Date _____

Sponsor Information

Name: _____ Telephone Number: _____

Department: _____ Room Number: _____
E-mail Address: _____
Position: _____

Signature of Sponsor _____Date: _____

26.6 Third Party Connection Agreement

This Third Party Network Connection Agreement (the "Agreement") by and between the Ministry of Gender Children and Social Protection (MGCSP), and _____ is entered into as of the date last written below ("the Effective Date").

This Agreement consists of this signature page and the following attachments that are in this Agreement by this reference:

1. Attachment 1: Third Party Network Connection Agreement Terms and Conditions
2. Attachment 2 Network Connection Policy
3. Attachment 3: Third Party Connection Request - Information Requirements Document
4. Attachment 4: Ministry of Gender Children and Social Protection (MGCSP) Non-Disclosure Agreement

This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Agreement.

Ministry of Gender Children and Social Protection (MGCSP) Authorized Signature _____	Third Party Company Authorized Signature _____
Name _____	Name _____
Date _____	Date _____

26.7 Non Compliance

This form should only be used to report observed or apparent noncompliance. Noncompliance is defined as failure or refusal to comply, as with a law, regulation or policy, or term of a contract.

SECTION I: INVESTIGATOR INFORMATION

Principal Investigator: _____

Building/Room No: _____

Department: _____

Phone: _____

E-Mail: _____

Contact Information

Name: _____

Address: _____

Phone: _____

E-Mail: _____

SECTION II: NONCOMPLIANCE INFORMATION

1. Provide an explanation of the facts surrounding the noncompliance, including a timeline of occurrence of noncompliance and discovery.

2. Provide an assessment of the increased risk (if any) to subjects resulting from the noncompliance.

3. Explain the corrective measures taken in response to the noncompliance and explain any preventive measures that will be taken to prevent the noncompliance from occurring in the future (if possible).

* Please attach any supporting documentation, such as an audit or monitoring report, etc.

SECTION III: INVESTIGATOR ACTION
Please indicate any actions that will be taken as a result of this report:

Statement of Principal Investigator. I have personally reviewed this report and agree with the above assessment.

Signature of Principal Investigator: _____ Date: _____

27. DEFINITION

- **Authorization / Authorized:** Official MGCSP approval and permission to perform a particular task.

- **Backup:** The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure, loss or theft etc.

- **Breach of Information Security:** The situation where MGCSP confidential or restricted information has been put at risk of unauthorized disclosure as a result of the loss or theft of the information or, through the accidental or deliberate release of the information.

- **Confidential information:** (As defined by the MGCSP Information Classification & Handling Policy) Information, which is protected by Ministry of Gender Children and Social Protection (MGCSP) and its information system are considered confidential information. The unauthorized or accidental disclosure of this information could adversely impact the MGCSP.

- **Defamatory:** False statement or series of statements, which affect the reputation of a person or an organization.

- **Electronic Media:** Any Information that has been created and is stored in an electronic format, including but not limited to software, electronic documents, photographs, video and audio recordings.

- **Encryption / Encrypt:** The process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorized persons.

- **Encryption Key:** A piece of data (parameter usually a password) used to encrypt/decrypt information.

- **Generic / Group Access Account:** An access account that is intended for use by a number of different people and not an individual user and as such is not derived from a single user's name.

- **MGCSP:** Ministry of Gender Children and Social Protection (MGCSP)

- **MGCSP Network:** The data communication system that interconnects different MGCSP Local Area Networks (LAN), Wide Area Networks (WAN) and Wi-Fi Wireless Networks.

- **MGCSP Server:** A computer on the MGCSP network used to provide network services and/or manage network resources.

- **Information:** Any data in an electronic format that is capable of being processed or has already been processed.

- **Information System:** A computerized system or software application used to access, record, store, gather and process information. Example, IMF/CASH TRANSFER SYSTEM/ETC.

- **Information Technology (I.T.) resources:** Includes all I.T. devices and equipment, computer facilities, networks, data & telecommunications systems, equipment and infrastructure, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the MGCSP.

- **Intellectual Property:** Any material, which is protected by copyright law and gives the copyright holder the exclusive right to control reproduction or use of the material.

- **Unit Director:** The individual a user reports directly to.

- **Ministry:** Throughout the document, Ministry has been used to reference the Ministry of Gender Children and Social Protection (MGCSP).

- **Mobile Computer Device:** Any handheld computer device including but not limited to laptops, tablets, notebooks, PDA's etc.

- **Network Administrators:** These are the individuals responsible for the day to day management of a MGCSP network domain. Also includes MGCSP personnel who have been authorized to create and manage user accounts and passwords on a MGCSP network domain

- **Network Domain:** A set of connected network resources (Servers, Computers, Printers, Applications) that can be accessed and administered as group with a common set of rules

- **Personal Use:** The use of the MGCSP's Information Technology (IT) resources for any activity(s), which is not MGCSP work-related.

- **Pornography / Pornographic**: The description or depiction of sexual acts or naked people that are designed to be sexually exciting.

- **Privacy:** The right of individual or group to exclude themselves or information about themselves from being made public.

- **Process / Processed / Processing:** Performing any manual or automated operation or set of operations on information including:

    1. Obtaining, recording or keeping the information;
    2. Collecting, organizing, storing, altering or adapting the information;
    3. Retrieving, consulting or using the information;
    4. Disclosing the information or data by transmitting, disseminating or otherwise making it available;
    5. Aligning, combining, blocking, erasing or destroying the information.

- **Removable Storage Device:** Any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external/portable hard drives.

- **Restricted Information:** (As defined by the MGCSP Information Classification & Handling Policy) highly sensitive confidential information. The unauthorized or accidental disclosure of this information would seriously and adversely impact the Ministry. Some examples of restricted information include:

    1. IMF/CASH TRANSFER UNIT database
    2. Check printing system
    3. Unpublished information
    4. Information marked classified
    5. Unpublished financial reports

- **Smart Device:** A handheld mobile computer device which is capable of wireless connection (via WiFi, 3G, 4G etc…), voice and video communication and, internet browsing.

- **Internet Video Hosting/ Sharing Websites:** Websites that allows users to upload video clips, which can then be viewed by other users. Including but not limited to YouTube, Yahoo Video, Google Video and My Video.

- **Blogging Websites:** Websites that allow a user to write an on-line diary (known as a blog) sharing their thoughts and opinions on various subjects

- **Software:** A computer program or procedure that enables a computer to perform a particular task.

- **System Administrators:** The individual(s) charged by the designated system owner with the day to day management of MGCSP information systems. Also includes the MGCSP personnel and third parties who have been authorized to create and manage user accounts and passwords on these applications and systems.

- **Third Party Commercial Service Provider:** Any individual or commercial company that have been contracted by the MGCSP to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the MGCSP.

- **Third Party Servers and Equipment:** Any servers or computer equipment used to store or host MGCSP information and/or information systems, which are not owned by the MGCSP.

- **Third Party Storage Facilities:** Any location or facility used to store MGCSP information, information systems and/or computer equipment, which is not owned or managed by the MFDP.

- **Users:** Any authorized individual who uses the MGCSP's I.T. resources.