NSWMA
IT Department
Jamaica's Beauty Is Our Duty
Email: ithelpdesk@nsma.gov.jm

National Solid Waste Management Authority - NSWMA

Information Technology Department ICT Policy

Restricted circulation – photocopying strictly prohibited

1.2	17.06.2019	Format Updates	O. Townsend		
1.1	26.03.2019	Recovered updates	M. Watson		
1.0	01.01.2019	First Draft	M. Watson		
Rev	**Date**	**Description of Revision**	**Issued by**	**Checked by**	**Approved by**

Table of Contents

Intentionally Left Blank

Foreword:

The National Solid Waste Authority (hereinafter after referred to as "NSWMA") through its Information and Communication Technology (ICT) Department, is committed to the responsible use of Information Technology resources, by providing a secure, reliable and available platform for information usage as well as the protection of its stakeholders in an effort to promote a safe and healthy ICT environment.

This Policy was created to raise awareness about the NSWMA's general expectations on the usage of ICT resources, the expected responsible behaviour of its users in areas, as listed below:

- Access Control;
- Bring Your Own Device;
- Acceptable Computer Usage;
- Data Backup;
- Email Usage;
- Internet Usage;
- Mobile Acceptable Usage;
- Software Usage;
- User Account and Password
- Social Media
- Account Termination; and
- Cellphone Policy.

The ICT Department believes that its ICT resources must be able to support all government approved systems, as well as provide strong ICT linkages to the regional WML companies, while supporting their infrastructure. In effectively discharging our duties, the ICT Department supports open source and vendor based solutions and believes in finding solutions related to saving and cost containment issues such as, but not limited to, digitizing of data, reduction on paper usage as well as assisting in the management of business processes such as tracking system, administration inventory management system and procurement systems.

The ICT Department is committed to researching emerging ICT trends and technology globally and seeks to bolster the capacity of the ICT team in order to meet the daily demands of the NSWMA in an efficient and effective manner to meet the NSWMA's mandates.

Intentionally Left Blank

Vision and Mission

Vision Statement:

The Vision of the Information & Communication Technology Department is to "provide strategic support to all NSWMA staff and affiliates in the most efficient and cost effective fashions.".

Mission Statement:

The Information and Communication Technology (ICT) Department is responsible for the innovation, implementation and advancement of Information and Communication Technology by:

- Aligning strategic objectives with that of NSWMA's Top management
- Aligning these objectives with modern ICT solutions;
- Managing and developing these ICT solutions;
- Providing Customer/Stakeholder Support;
- Providing Stakeholder Consultations; and
- Facilitating communication links between our locations; and
- Creating bridges to any gaps in communicating with our stakeholders.

Introduction:

Computer information systems (including network and its related technologies), are an integral part of business within any organization, as they form the backbone to the successful implementation of projects and programs. The NSWMA is no different. The NSWMA-owned computer systems are utilized in many areas such as, direct administrative, professional development, research and communication. These functions are heavily reliant on computing and networking technology to accomplish their Departments' goals based on the overall strategic direction of the NSWMA.

Overview of the NSWMA's ICT System:

The NSWMA's main offices are situated at 61 Half-Way-Tree Road with the Regional offices are dispersed geographically throughout the country for each zone of operation, namely WPM, NEPM, SPM and MPM.

The NSWMA's communication platform is supported by Cloud VPN backbone controlled by Firewalls at each main location. With approximately three hundred

(300) users, supported at five (5) different offices, the 6 member ICT has its hands full with technical requests on a daily basis.

The NSWMA therefore has made substantial investment in its human and financial resources to create and maintain computer systems which would enhance internal processes, in order to assist in accomplishing its mandate. The Information and Communication Technology (ICT) Department is charged with the responsibility of supporting and monitoring the NSWMA 's computing and networked resources, hereinafter referred to as Information Technology (IT) Assets.

The NSWMA provides a wide variety of computing and networking resources to staff employed by the NSWMA. Access to computers, computing systems and networks owned by the NSWMA is a privilege which imposes certain responsibilities and obligations which is granted subject to the Staff Orders, HR and ICT policies. All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources including wireless services.

With this in mind, an ICT Policy is purposed to guide the use of, and assist in the protection of the NSWMA's computer systems, its network infrastructure and its related periphery resources. The purpose of this policy is to promote the efficient, ethical and lawful use of the NSWMA's computer and network resources. This policy document (hereafter referenced as the NSWMA ICT Policy for the) forms the framework for addressing policy and operational procedures in deploying securing the NSWMA's ICT systems.

SCOPE:

The ICT Policy document will be used to inform and guide NSWMA users on the of the IT Assets and ICT Systems.

AUDIENCE:

The ICT Policy is written specifically for the staff/users who utilize the NSWMA's ICT System and IT Assets, whether initiated from a computer and/or network device located on or off the NSWMA's compound.

INCIDENT HANDLING:

Inappropriate use of the NSWMA's computer facilities is divided essentially into two main areas; illegal activity and activity in breach of the NSWMA's Security Policy.

Where illegal activities are suspected, the Director of ICT must be notified immediately, who will in consultation with Executive Management then decide on the appropriate course of action. An investigation authorized by Executive Management may then proceed.

Where activities are in breach of the NSWMA's rules, the Director of ICT must be notified immediately, who will then decide on the appropriate course of action in consultation with the Executive Director.

ICT Department RESPONSIBILITIES:

- Controls access to the NSWMA's network and its Internet connection**.**
- Does not take responsibility for the corruption, physical damage or theft of personal equipment within the NSWMA's environs.
- Does not service Internet Protocol (IP) Phones, printers, scanners, cell phones, plotters or tablets.
- Is exclusively responsible for installing and supporting SOFTWARE on ALL of the NSWMA computers. These responsibilities extend to:
    - ✓ Office desktop computers
    - ✓ Company laptop computers
    - ✓ Servers
    - ✓ Smart phones and Tablets (where applicable)
- Is responsible for the assignment of all IT assets to NSWMA users' based on situational analysis, subsequent to an official instruction from The NSWMA's HR Department via The IT Help Desk.
- Is responsible for the sanitization of all the NSWMA -owned electronic devices and computer systems in the various units prior to removal from the NSWMA.

- Monitors and maintains traffic and logs for the following purposes:
  - ✓ To maintain and enforce network security
  - ✓ To maintain and monitor the integrity of computer systems
  - ✓ To check for misuse of resources
  - ✓ To gather usage statistics
- Maintains Personal Computers (PC)
  - ✓ This will be done internally by the NSWMA ICT staff members when the computers are void of warranty, otherwise an external technician may be contracted to service them.
- Reserves the right to restrict or limit the usage of the NSWMA 's network. The restriction will be on the basis of what it has deemed to be a realistic threat or causing sufficient attrition of network resources (bandwidth) and is done without prejudice or malice.
- Monitors all software licenses owned by the NSWMA and them only.
- Will undertake monitoring of a variety of information as it is the provider of network infrastructure and core computer services for the NSWMA.
- Will remove unauthorized operating systems which are installed on the NSWMA's network.
- Will NOT routinely monitor or inspect
  - ✓ That part of any log which may be related to an individual
  - ✓ The contents of electronic mail folders
  - ✓ The contents of any personal files stored
- If requested, however (for investigative purposes), will provide access to:
  - ✓ That part of any log which may be related to an individual
  - ✓ The contents of electronic mail folders
  - ✓ The contents of any personal files stored

FAILURE TO COMPLY WITH NSWMA RULES, POLICIES AND PROCEDURES:

The failure to comply with the NSWMA rules, policies and procedures is likely to result in formal action being considered under NSWMA's Disciplinary Procedure Manual. In appropriate cases, the matter may be reported to the police and or any other relevant compliance, investigative or prosecuting authority.

Intentionally Left Blank

Policy

*A **policy** is a principle to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol.*

Intended effects

The intended effects of a policy vary widely according to the organization and the context in which they are made. Broadly, policies are typically instituted to avoid some negative effect that has been noticed in the organization, or to seek some positive benefit.

Unintended effects

Policies frequently have side effects or unintended consequences. Because the environments that policies seek to influence or manipulate are typically complex adaptive systems (e.g. governments, societies, large companies), making a policy change can have counterintuitive results.

1. ACCESS CONTROL POLICY

1.2. Statement of Policy:

The NSWMA implements access control across its networks, ICT systems and services in order to provide authorized, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Technology Policy.

Access control systems are in place to protect the interests of all authorized users of the NSWMA ICT systems by providing a safe, secure and accessible environment in which to work.

1.2. Scope of This Policy:

The Policy applies to all staff members using the network and Internet at the NSWMA. This policy covers all the NSWMA networks, communications rooms, ICT systems, data and authorized users.

1.2. Definitions:

The management of access to system grants authenticated users access to specific resources based on company policies and the permission level assigned to the user or user group. Access control often includes authentication, authorization and accounting, which proves the identity of the user or client machine attempting to log in; determines what is to be accessed; and the logging of all activities carried out with each user account.

1.2. Introduction:

Access control systems are in place to protect the interests of all authorized users of the NSWMA ICT systems by providing a safe, secure and accessible environment in which to work.

1.4.1. Principles:

the NSWMA will provide all employees, and contracted third parties with on-site access to the information required to effectively operate out their responsibilities in as effective and efficient manner as possible.

1.4.2. Generic identities

Generic or group IDs shall not normally be permitted as means of access to the NSWMA data, but may be granted under exceptional circumstances if sufficient other controls or access are in place.

1.4.3. Privileged accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default. Authorisation for the use of such accounts shall only be provided explicitly, upon written request to the Director ICT any of his designates, and will be documented by the system owner.

1.4.4. Least privilege and need to know

Access rights will be accorded following the principles of least privilege and need to know.

1.4.5 Maintaining Data Security Levels

Every user should understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to their sensitivity.

Users electing to place information on digital media or removable storage devices or maintaining a separate database are advised by IT team only do so where such an action is in accord with the information's security classification. Users are consequently responsible in such situations for ensuring that appropriate access to the data are maintained in accord with the Information Security Policy and any other contractual obligations they may have to meet.

Users are obligated to report instances of non-compliance to the NSWMA via email to the Director ICT or any member of the ICT Team.

1.5 Access Control Authorisation:

1.5.1 User Accounts:

Access to the NSWMA ICT resources and services will be given through the provision of a unique user account and complex password.

1.5.2 Staff User Accounts:

Staff user accounts can only be requested in writing, by departmental managers to the Director ICT or his assigned designate. No access to any the NSWMA staff IT resources and services will be provided without prior authentication and authorization of a user's the NSWMA account.

1.5.3 Third Parties:

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

1.5.4 Passwords:

Password issuing, strength requirements, changing and control will be managed through formal processes. Password issuing will be managed by the ICT Team. Password length, complexity and expiration times will be controlled. Password changing can be performed on the NSWMA laptops by the ICT Team.

1.5.2 Access to Confidential, Restricted and Internal Use information:

Access to 'Confidential', 'Restricted' and 'Internal Use' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within the NSWMA and administered by IT Team.

1.6. Policies and guidelines for use of accounts:

Users are expected to become familiar with and abide by the NSWMA policies, standards and guidelines for appropriate and acceptable usage of the networks and systems which also includes the acceptable use policy.

1.6.1 Access for remote users:

Access for remote users shall be subject to authorization by Director ICT and his appointed designate and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system without consent from the Director ICT or his assigned designate.

1.7. Access Control Methods:

Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, the NSWMA login rights, database access rights, encryption and other methods as necessary.

Access control applies to all the NSWMA -owned networks, servers, workstations, laptops, mobile devices and services run on behalf of the NSWMA.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within the NSWMA domains.

1.7.1 Further Policies, Codes of Practice, Procedures and Guidelines:

This policy sits beneath The NSWMA overarching ICT Policy. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available. All staff, students and any third parties authorised to access The NSWMA network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

1.8. Review and Development

This policy shall be reviewed and updated regularly by the ICT Team as appropriate to ensure that it remains appropriate in the light of any relevant changes to organisational policies or contractual obligations.

Intentionally Left Blank

2. BRING YOUR OWN DEVICE (BYOD) POLICY

2.2. 2.1 Statement of Policy:

The most common challenge is that users do not recognize that mobile devices represent a threat to IT and data security. As a result they often do not apply the same security and data protection guidelines as they would on other devices such as desktop computers.

The second challenge is that when users provide their own devices they often give greater weight to their own rights on the device than to their employer's need to protect data.

2.2. Scope of This Policy:

This outline policy gives a framework for securing mobile devices and should be linked to other policies which support The NSWMA posture on IT and data security.

All mobile devices, whether owned by the NSWMA or owned by employees, that have access to corporate networks, data and systems, including corporate IT-managed laptops. This includes smartphones and tablet computers.

2.2. Definitions:

2.3.1 Mobile Device:

Any handheld or portable computing device including running an operating system optimized or designed for mobile computing, such as Android, Blackberry OS (RIM), Apple's IOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

2.3.2 PDA:

PDA is a handheld device that combines computing, telephone/fax, internet and networking features.

2.3.3 Sensitive Information:

Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on the NSWMA interests, the conduct of the NSWMA programs or the privacy to which individuals are entitled.

2.3.4 PIN:

Personal Identification Number: This can be any combination of numbers (usually a minimum of four) that is used to unlock a device.

2.3.5 Encryption:

The use of software or hardware to make data unreadable unless the device is presented with the correct password or PIN. Most Mobile Devices include this feature but require the user to enable it.

2.3.6 Remote Wipe:

The ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.

2.3.7 Virus:

Virus is a computer program that is usually hidden within another seemingly innocuous program that has the function of stealing or destroying data or causing any number of unwanted system behaviors.

2.3.8 Malicious Software:

Often called malware, this is software designed to disrupt computer operation, gather Sensitive Information, or gain unauthorized access to computer systems.

2.3.9 Anti-virus Software:

Software designed to detect and/or remove Malicious Software and Viruses from a computer system.

2.3.10 Strong Password:

Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can’t be one of 15 previous passwords. Strong Passwords do not include phrases, names, or other types of dictionary words.

2.3.11 Security Patch:

A patch is a fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most Mobile Devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

2.2. Introduction:

The NSWMA grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. The NSWMA reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of The NSWMA's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The NSWMA employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

2.2. Acceptable Use:

- The NSWMA defines acceptable business use as activities that directly or indirectly support the business of The NSWMA.
- The NSWMA defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Devices’ camera and/or video capabilities are/are not disabled while on-site.
- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities.
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- The NSWMA has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

2.2. Devices and Support:

- Smart phones including but not limited to iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

2.2. Security:

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- After five failed login attempts, the device will lock. Contact IT to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphone and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.
- Smartphone and tablets belonging to employees that are for personal use only are allowed to connect to the network with permission from the Managing Partner or IT Team.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

2.5.3 Risks/Liabilities/Disclaimers

- While the ICT Department will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.

- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The NSWMA reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Intentionally Left Blank

3. ACCEPTABLE USAGE POLICY

3.2. Statement of Policy:

The NSWMA is committed to provide Internet Access and network services in a professional work environment.

This policy is intended to inform all staff of the NSWMA of their accessibility rights to ICT resources and the expectations and acceptable behaviors when they are using same.

3.2. Scope of This Policy:

The Computer Use Policy applies to use of all The NSWMA computing resources. Additional computer and network use policies and terms and conditions may be in place for specific electronic services offered by the organisation.

3.2. Definitions:

Computer System: A system of interconnected computers that share a central storage system and various peripheral devices such as a printers, scanners, or routers. Each computer connected to the system can operate independently, but has the ability to communicate with other external devices and computers.

3.2. Introduction:

This policy is intended to protect the technological infrastructure of the NSWMA, usage of NSWMA assigned devices, and separation of Official and Private Use. Limited exceptions to the policy may occur due to variations in devices and platforms.

3.4.1 Rights and Responsibilities:

Computers and networks can provide access to resources on and off the organisation, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

The NSWMA employees may have rights of access to information about themselves contained in computer files, as specified in the Access to Information Act1. Files may be subject to search under court order. In addition, system administrators may access user files as required to protect the integrity of computer systems. For example, following organizational guidelines, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

The NSWMA's staff are assigned various ICT devices from Computer Systems, Tablet PC to Mobile Phones to enhance the communication between internal and external stakeholders. The devices are to be used for official government use and it is recommended that the assigned NSWMA Staff use this device for the work of the NSWMA.

3.5. Existing Legal Context:

Misuse of computing, networking, technological devices or information resources may result in the restriction of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable the NSWMA policies, procedures, or contractual agreements. Complaints alleging misuse of the organizations computing and network resources will be directed to those responsible for taking appropriate disciplinary action.

[1] http://www.ati.gov.jm/

3.6. Examples of Misuse:

Examples of misuse include, but are not limited to, the activities in the following list.

- Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account owner.
- Using the NSWMA Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Deliberately wasting computing resources.
- Using electronic mail to harass others.
- Masking the identity of an account or machine.
- Posting materials on electronic bulletin boards, the NSWMA Intranet that violate existing laws or the NSWMA codes of conduct.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Activities will not be considered misuse when authorized by appropriate the NSWMA officials for security or performance testing.

3.7. Appropriate Use:

As a matter of service, the NSWMA extends to its staff the privilege to use its computers, mobile technologies and network infrastructure. When you are provided access to our organisations network, you are enabled to send and receive electronic mail messages globally, share in the exchange of ideas through electronic news groups, and use Web browsers and other Internet tools to search and find needed information.

The Internet is a very large set of connected computers, whose users make up a worldwide community. In addition to formal policies, regulations, and laws which govern your use of computers and networks, the Internet user community observes informal standards of conduct. These standards are based on common understandings of appropriate, considerate behavior which evolved in the early days of the Internet, when it was used mainly by an academic and highly technical community. The Internet now has a much wider variety of users, but the early codes of conduct persist, crossing boundaries of geography and government, in order to make using the Internet a positive, productive, experience. You are expected to comply with these informal standards and be a "good citizen" of the Internet.

3.8. Enforcement:

Penalties may be imposed under one or more of the following:

Minor infractions of this policy or those that appear accidental in nature are typically handled informally by electronic mail or in-person discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

Infractions by employees may result in the temporary or permanent restriction of access privileges.

Offenses which are in violation of local laws may result in the restriction of computing privileges, and will be reported to the appropriate officers in the NSWMA and law enforcement authorities if required.

3.9. Standardization of the NSWMA IT Assets and Infrastructure:

The aim of the ICT Department is to collaborate with all the Departments within the NSWMA to procure, implement and standardize IT assets and infrastructure. This is with an aim to increase and improve communication among the assets, and to encourage staff to be knowledgeable with the standard implemented technology. Standardization will work to reduce compatibility issues and problems which may arise when replacement parts are required. Standardization will also reduce the burden on the IT staff in respect to troubleshooting, updating and patching.

3.9.1 Minimum Technological Requirement for the NSWMA's:

The NSWMA has adopted the specifications which will be subject to change. This document must be created yearly to match based on the NSWMA's user needs and requirements and held by the ICT Department.

Intentionally Left Blank

4. DATA BACKUP POLICY

4.2. Statement of Policy:

The NSWMA is committed to provide Internet Access and network services in a professional work environment.

This policy is intended to protect The NSWMA data and its electronic information and ensure availability as required by officers of the NSWMA.

This policy is designed to protect data in the organization, while ensuring and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

4.2. Scope of This Policy:

The Computer Use Policy applies to protection of all the NSWMA computing resources. This policy applies to all equipment and data owned and operated by or on behalf the organization.

4.2. Definitions:

Backup: The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive: The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

Restore: The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

4.2. Introduction:

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

4.5. Timing:

Incremental backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, manual backups are not performed on Friday, they shall be done on Saturday.

4.6. Monthly Backups:

Every month, monthly backups are stored on external hard drives

4.7. Responsibility:

The ICT Director shall delegate a member of the ICT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

4.8. Testing:

The ability to restore data from backups shall be tested at least once per month.

4.9. Data Backed Up:

Data to be backed up include the following information:

1. User data stored on the hard drive.

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server

4. Production database server
5. Domain controllers
6. Test database server
7. Test web server

4.10. <u>Archives</u>:

Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

4.11. <u>Restoration:</u>

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

4.12. <u>Tape Storage Locations:</u>

Offline tapes used for nightly backup shall be stored in an adjacent building in a fireproof safe. Monthly tapes shall be stored across town in our other facility in a fireproof safe.
This policy may contain descriptions about how various systems and types of systems are backed up such as Windows systems.

Intentionally Left Blank

5. E-MAIL USAGE POLICY

5.2. Statement of Policy:

The purpose of the NSWMA email system is to provide an efficient, speedy and effective tool for the facilitation of official the NSWMA communications among the NSWMA staff members and between the NSWMA and its external stakeholders. Though it is not encouraged, the limited use of the e-mail service for incidental personal purposes is permitted. Staff members should particularly note that prior to, or upon separation, the NSWMA reserves the right to peruse .PST or any of the NSWMA account along with other files which are recorded upon assigned staff computers in an effort to disaggregate official mails from personal mails for the purpose of business continuity.

The protection of the NSWMA confidential information is a statutory and contractual obligation which is imposed upon all the NSWMA employees and advances in information technology must not compromise this.

The NSWMA is committed to a consistent approach to risk management and reserves the right, at any time, to take such steps as it may deem appropriate to this end. This applies to protecting confidentiality, availability and integrity of The NSWMA information systems, any the NSWMA confidential information, as well as the reputation of the Organization and its employees.

The NSWMA is also committed to the promotion of innovative practices within a learning organization.

5.2. Scope of This Policy:

This policy applies to the users of all electronic mail and computer based electronic messaging systems which are in use within the NSWMA.

5.2. Definitions:

A system for sending messages from one individual to another via telecommunications links between computers or terminals using dedicated software.2

5.2. Introduction:

The NSWMA provides an e-mail facility to all of its employees. However, the continuing growth in the use of email, together with the expansion of potential recipients through connection to the Internet, means that certain standards and guidelines must be laid down identifying the behavior and uses which are acceptable to the NSWMA when e-mails are being sent by the staff members.

This policy provides guidance, together with formal statements of the position of the NSWMA with regard to certain categories of e-mail use.

It also aims to assist staff in understanding the role of e-mail as an office tool, and to exercise appropriate judgment in using that tool. It builds upon existing the NSWMA organizational policies and procedures, notably those relating to standards and guidelines for the use of The NSWMA computers and network.

5.2. Application:

This policy applies to staff at all grades and levels within the NSWMA who have access to e-mail facilities via The NSWMA e-mail facility.

5.2. Use of E-mail:

The purpose of the NSWMA email system is to provide an efficient, speedy and effective tool for the facilitation of official the NSWMA communications among the NSWMA staff members and between the NSWMA and external stakeholders. Though it is not encouraged, the limited use of the e-mail service for incidental personal purposes is permitted. Incidental personal use excludes use requiring

[2] dictionary.reference.com/browse/**e-mail**

substantial expenditure of time, for profit or use which would otherwise violate any established policy or management arrangement of the NSWMA , with due regard to employee time, commitments and The NSWMA equipment.

E-mail may not be used to infringe the copyright or other intellectual property rights of parties, to distribute any defamatory, sexual, sexist, racist or fraudulent material, or harassing messages, or otherwise to engage in any illegal or wrongful conduct.

The NSWMA distribution lists are not to be used, if e-mails are be sent to external recipients for any personal business outside of the NSWMA.

5.2. Practice Guidelines:

E-mail is to be treated as a permanent written communication.

Every staff member to whom a computer is assigned must ensure that Outlook is set to check regularly for new messages. Emails are to be read at least four [4] times daily… i.e. twice in the morning and twice in the evening or approximately once every two hours, **once the staff member is in office**.

Intentionally Left Blank

6. INTERNET USAGE POLICY

6.2. Statement of Policy:

The NSWMA is committed to provide Internet Access in a professional work environment. This policy is intended to inform all staff of the NSWMA of their accessibility rights to the Internet and the expectations and acceptable behaviors when they are using same.

6.2. Scope of This Policy:

The Policy applies to all staff members using the Internet at the NSWMA.

6.2. Definitions:

Internet Usage includes, but is not limited to, the following:

- Email
- Accessing Web Sites
- Accessing News Group (Jamaica Observer, Gleaner and Herold)
- Chat
- Files sharing/upload/download
- Telnet

6.2. Introduction:

The NSWMA staff has been entrusted with access to the internet and by such must take the necessary steps to ensure that it is properly managed within the parameters of its intended use.

6.2. Monitor Internet Usage:

The NSWMA can and will monitor all Internet usages. All Internet activities can and will be logged for further review. This is to ensure that all Internet users adhere to The NSWMA policy.

Compliance Audits will be conducted by the ICT Department periodically.

6.2. Activities can be Blocked:

The NSWMA can and will block certain Internet activities that are deemed unsuitable and/or unacceptable for the Office environment.

6.2. Activities not Permitted:

The following activities are deemed unproductive by the NSWMA and are therefore NOT permitted:

- Circulation of foul/obscene/offensive language/material
- Harassing or insulting others
- Violation of laws (copyright and others)
- Hacking or damaging computers
- Misrepresenting yourself/facts or others

6.2. Object-able Material:

Users should not access/upload/download/circulate materials that can be deemed object able to other employee. These include, but are not limited to material such as jokes, harassments or discrimination of a certain group of people based on:

- Sex
- Race
- National origin
- Ethnicity
- Age
- Physical Ability/Appearance
- Sexual Orientation
- Religion
- Political Affiliation
- Marital/Family/Social Status
- Language
- Disability

- Medical Status/Conditions
- Or any other action that is prohibited by law

6.2. Confidential/Sensitive Material:

Users should not upload/save/circulate The NSWMA confidential and/or sensitive material to the public or any locations that are considered not appropriate or insecure.

6.2. Disciplinary Action:

All Employees are advised and expected to adhere to this Internet Usage Policy. Internet misuse can result in disciplinary action being taken as per The NSWMA Disciplinary Code.

Deal with e-mails promptly by way of:

- Reply;
- Print and forward to appropriate persons;
- Delete; and
- Save 'Word' attachments to My Documents or the appropriate folder on hard drive.

As far as is practicable and save for exceptional circumstances, the use of the NSWMA e-mail to send all internal memoranda, circulars, etc. is recommended. This is often more cost effective and efficient than photocopying and posting.

E-mails which are received with an attachment from an unknown address must be checked out with the appropriate virus scan or if you are unsure contact the ICT Department before opening. Indeed, any uncertainties regarding incoming e-mails should be queried with the ICT Department.

6.2. User Responsibilities:

Employees are personally responsible for any e-mail that is sent from their respective e-mail accounts. To ensure that unauthorized messages are not sent, all employees should ensure that during any unattended period, the terminal is locked and, where appropriate, any communication session is closed.

All employees have a duty to take appropriate care of their passwords. This includes not providing passwords to any third party for any reason.

Users are reminded that the un-authorized use of another person’s Computer ‘login’ password constitutes a breach of security. If problems arise, the ICT Department will be able to provide support to solve the issue.

All employees are required to promptly report any e-mails which are received that contain defamatory, sexual, sexist or racist material to the ICT Director or his designate with follow-up in writing.

6.2. Human Resource Management:

In the event that an employee is to be separated from the Organization, the rights of the organization are reserved to remove full access to an e-mail account from that member of staff.

For security purposes, only one (1) person from the ICT Department should have access to the .PST files file and a copy should be held by the Snr. HR Director in a sealed envelope.

In the event that a staff member is separated or is to be separated from the organization, the NSWMA reserve the right to peruse his/her .PST and other computer files in an effort, *inter alia*, to disaggregate official mails and files from personal mails and files.

6.2. E-mail Disclosure:

All e-mails being sent by any the NSWMA employee must be affixed with the below signature. The Director ICT Department will ensure that it is automatically affixed to all e-mails.

<NAME>
<POSITION>
NSWMA of Economic Growth and Job Creation
The Towers, 25 Dominica Drive, Kingston 5
Jamaica W.I.
<CUG>
<Telephone:>
<Email>

Confidential, Privileged, Proprietary and/or Sensitive Information This e-mail message and any document which is attached to it are intended solely for the use of the person or persons to whom the message is addressed. The message and/or its attachments may contain information which is confidential, privileged, proprietary and/or sensitive in nature. If you have received this e-mail message in error, you are hereby advised that any further dissemination, distribution, publication and/or copying of same is prohibited. If you believe that you have received this e-mail in error, please contact the sender by telephone and delete the message and its attachments from your system immediately. Please also note that we cannot guarantee that this message and its attachments, if any, are virus free or have been intercepted or amended.
THANK YOU FOR YOUR CO-OPERATION.
Please consider the environment before printing this email

6.2. Configuring of Services:

Only the ICT Department or any 3rd Party technical person, recommended by the ICT Director and his designates, are allowed to configure the the NSWMA ICT infrastructure. Once controls are set on assigned computers, staff members are not permitted to re-adjust the set controls.

Intentionally Left Blank

7. MOBILE ACCEPTABLE USAGE POLICY

7.2. Statement of Policy:

The most common challenge is that users do not recognize that mobile devices represent a threat to IT and data security. As a result they often do not apply the same security and data protection guidelines as they would on other devices such as desktop computers.

The second challenge is that when users provide their own devices they often give greater weight to their own rights on the device than to their employer's need to protect data.

7.2. Scope of This Policy:

This outline policy gives a framework for securing mobile devices and should be linked to other policies which support your organization's posture on ICT and data security.

This refers to all mobile devices (Smartphone and tablet computers), whether owned by the NSWMA or owned by an employee, that have access to corporate networks, data and systems, excluding corporate ICT-managed laptops.

7.2. Definitions:

Mobile Device: Any handheld or portable computing device including running an operating system optimized or designed for mobile computing, such as Android, Blackberry OS (RIM), Apple's iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

PDA: A handheld device that combines computing, telephone/fax, internet and networking features.

Sensitive Information: Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on the NSWMA interests, the conduct of the NSWMA programs or the privacy to which individuals are entitled.

PIN: Personal Identification Number: This can be any combination of numbers (usually a minimum of four) that is used to unlock a device.

Encryption: The use of software or hardware to make data unreadable unless the device is presented with the correct password, swipe or PIN. Most Mobile Devices include this feature but require the user to enable it.

Remote Wipe: The ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.

Virus: A computer program that is usually hidden within another seemingly innocuous program that has the function of stealing or destroying data or causing any number of unwanted system behaviors.

Malicious Software: Often called malware, this is software designed to disrupt computer operation, gather Sensitive Information, or gain unauthorized access to computer systems.

Anti-virus Software: Software designed to detect and/or remove Malicious Software and Viruses from a computer system.

Strong Password: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords. Strong Passwords do not include phrases, names, or other types of dictionary words.

Security Patch: A fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most Mobile Devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

7.2. Introduction:

The NSWMA grants its employees the privilege of purchasing and using Smartphones and tablets of their choosing at work for their convenience. The NSWMA reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of The NSWMA data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. T NSWMA employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the NSWMA network.

7.2. Acceptable Use:

- The NSWMA defines acceptable business use as activities that directly or indirectly support the business of the NSWMA.
- The NSWMA defines acceptable personal use on the organisations time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Devices' camera and/or video capabilities are/are not disabled while on-site.
- Devices may not be used at any time to:
  - Store or transmit illicit materials;
  - Store or transmit proprietary information belonging to another the NSWMA ;
  - Harass others; and
  - Engage in outside business activities.
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
- Employees may use their mobile device to access the following the NSWMA -owned resources: email, calendars, contacts, documents, etc.
- **The NSWMA has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.**

7.6. Devices and Support:

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Connectivity issues are supported by ICT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

- Devices must be presented to ICT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

7.7. Security:

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the organisations network.
- The NSWMA strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- The device must lock itself with a password, swipe or PIN if it's idle for five minutes.
- After five failed login attempts, the device will lock. Contact ICT to regain access.
- Rooted (Android) or jail-broken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets that are not on The NSWMA list of supported devices are/are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are allowed to connect to the network with permission from the Managing Partner or IT Team.
- Employees' access to the NSWMA data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of The NSWMA data and technology infrastructure.

7.8. Risks/Liabilities/Disclaimers:

- While ICT Department will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, etc.
- The NSWMA reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the NSWMA within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to The NSWMA acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of the NSWMA and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The NSWMA reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Intentionally Left Blank

8. SOFTWARE USAGE POLICY

8.2. Statement of Policy:

The NSWMA is committed to providing software for usage within in a professional work environment.

This policy is intended to inform all staff of the NSWMA of their accessibility rights to the computer system, its software's and the expectations and acceptable behaviors when they are using same.

8.2. Scope of This Policy:

Specific information on the use and copying of computer software acquired by purchase or gift, and guidance on the legitimate property rights of those who hold the copyrights.

8.2. Definitions:

- **Backup**: The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- **Archive:** The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
- **Restore:** The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

8.2. Introduction:

The NSWMA recognizes the importance of the legal and ethical use of software assets. This document provides guidelines for employees to follow to ensure that we are both legal and ethical in the use of our software assets. All software assets are for business use only and should not be used by employees for personal interests. ***The NSWMA Policy on Use of Software***

8.2. General Policies:

The NSWMA has purchased fully licensed copies of computer software from a variety of publishers and vendors. Licensed and registered copies of software programs are placed on computers within the NSWMA and appropriate backup copies made in accordance with the licensing agreements and the NSWMA policies. No other copies of this software or its documentation can be made without the express written consent of the software publisher and the NSWMA.

8.2. Software from Other Sources:

The NSWMA will provide copies of legally acquired software to meet all legitimate needs in a timely fashion and in sufficient quantities for all required computers. The use of software obtained from any other source could present security and legal threats to the NSWMA, and such use is strictly prohibited.

8.2. Additional Copies:

In some cases, the license agreement for a particular software program may permit an additional copy to be placed on a portable computer or home computer provided only one user uses both installations. Employees will not make such additional copies of software or documentation for the software without the approval of the NSWMA ICT Department. When legal, approval will be granted for such installations when there are valid business reasons.

8.2. Unauthorized Copies:

The unauthorized duplication of copyrighted software or documentation is a violation of the law and is contrary to established standards of conduct for the NSWMA employees. Employees, who make, acquire or use unauthorized copies of computer software or documentation will be subject to immediate discipline up to and including immediate termination of employment.

8.2. Internal Controls:

The NSWMA reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorized copies of software. These controls may include periodic assessments of software use, announced and unannounced audits of the NSWMA computers to assure compliance, the removal of any software found on the NSWMA property for which a valid license or proof of license cannot be determined, and disciplinary actions, including termination, in the event of employee violation of this policy.

Intentionally Left Blank

9. USER ACCOUNT AND PASSWORD POLICY

9.2. Statement of Policy:

The NSWMA implements usernames and passwords to all its users to access the NSWMA Technological and network infrastructure. This policy is designed to provide the rules governing authentication to the users of these systems and there overall responsibility as users.

9.2. Scope of This Policy:

The Policy applies to all staff members using the network and Internet at the NSWMA. This policy covers all the NSWMA networks, communications rooms, ICT systems, data and authorised users.

9.2. Definitions:

Username: A username is a name that uniquely identifies someone on a computer system.

Password: A sequence of alphanumeric and special characters entered in order to gain access to a computer system or resource.

System Administrator: A person who is responsible for properly maintaining a server, workstation, or other networked device.

VPN: Virtual Private Network. A technology provides secure communications from remote locations to a known location at the NSWMA, typically over the public Internet. However, VPNs are not inherently about security or performance, but rather that they provide a "tunnel" on top of some other network in support of a given customer or client community.

9.2. Introduction:

This policy is intended to protect the security and integrity of The NSWMA data and technological infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

9.2. Effective Passwords:

All the NSWMA user accounts will be protected by effective passwords. An effective password is both strong and protected. Strong passwords have at least a specified minimum number of characters, are a combination of alphabetic, numeric and special characters, and are not common dictionary words. Account holders and system administrators, acting as account/password custodians, will protect the security of those passwords by managing passwords in a responsible fashion.

9.2. Rationale:

Account holders are held responsible for all activities associated with their accounts. As such, the strength and protection of the password is critical to ensuring that unauthorized activity does not become associated with a person's account. Each computer user is responsible for his or her use of technology at the NSWMA. The integrity and secrecy of an individual's password is a key element of that responsibility.

9.2. Updating Passwords:

As time passes from a password update, the probability that a password has been compromised increases. This probability goes up because of the risk of silent compromise of someplace where the password was entered (keystroke logger) or accidental use over an insecure path (for example, VPN's that fail "open" leading you to think you are encrypted when you are not!).

9.2. Implementation: Account holders should:

- Create a strong password.
- Change the password as frequently as needed to ensure security for the resources computers, data, etc. under their control. As a matter of practice, ICT Department suggests changing passwords at least every quarter.
- Safeguard their password. For example, individuals should not write down or store the password on paper or on a computer system where others might acquire it.
- Never share their password. We recognize there may be times when people need to have someone do something on their behalf, when work is being delegated, and lack of access to an account might impede business. That said, we want to emphasize that when you give someone your password, they may take actions in your name that you might not be aware of, might not approve of, but may be held responsible for depending on the nature of the activity.
- Never reuse the NSWMA user name and password for external services, be they related to the NSWMA business or of a personal nature.
- Change your password immediately if they know or suspect that it has been guessed, stolen, intercepted, or otherwise compromised. Contact IT Team for further guidance and assistance if this occurs.

System administrator is expected to:

- Store account passwords such that they cannot be produced on demand under any circumstances.
- Prevent, or take steps to reduce the likelihood of, the exposure of any clear text account passwords that an IT application, system, or other service has received for purposes of authentication.

Just as security and privacy risks evolve, password standards need to evolve to meet those risks. The NSWMA account password standard (see References below) establishes requirements for:

- Password minimum length
- Composition

- Password aging
- Reuse of old passwords

At initial account creation, a password is selected and tested against the then current standards. Passwords do not expire. Authorizations may expire at the discretion of a resource/service provider. ICT team may notify account holders of potentially weak -- or out of standard -- passwords based solely on ICT Teams records of when a particular password was last changed.

Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to that application.

9.2. Implications:

Ultimately, account security depends on users following the password policy. Therefore, educating account holders about the policy is essential to preventing unauthorized use of accounts.

Hackers and other Internet criminals are constantly evolving new strategies for breaking through security measures, so ICT Department must remain informed about current best practices regarding passwords.

Intentionally Left Blank

10. Social Media POLICY

10.1. Statement of this Policy

This policy is designed to provide the rules governing the use of Social Media within the NSWMA and the overall responsibility as users.

10.2. Scope Policy Statement

The policy is being developed is focused on employee's use of social media during working hours and the ownership of business contacts made during the course of employment.

10.3. Definition

Social media are computer-mediated tools that allow people to create, share, or exchange information, career interests, ideas, and pictures/videos in virtual communities and networks[3].

10.4. Introduction:

The term "social media" includes all means of communicating, creating, sharing posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, web journal or diary, personal web site/page, social networking (such as Facebook, MySpace, Twitter, Instagram, Linkedln, among others…), web bulletin board, or a chat room whether or not associated or affiliated with the NSWMA, as well as any other form of electronic communication.

10.5. Guidelines:

Social Media should therefore enable the NSWMA's employees to communicate with each other and an external audience on various topics. Moreover, some employees are asked to tweet about a NSWMA event in order to garner support

[3] https://en.wikipedia.org/wiki/Social_media

and attendance. The NSWMA, through its Public Relations Department/Unit or an Authorized individual is the **only** Unit/Personnel allowed to send out/release information regarding the NSWMA. As such postings to the NSWMA's official Facebook page, LinkedIn or Twitter account by unauthorised users are strictly prohibited. Failure to adhere to this policy will result in disciplinary actions and/or dismissal as outlined in the HRM Procedural Manual and/or the Staff Orders. For entities, such as the **MET Services** that falls under the purview of the NSWMA use of social media shall be governed by the Guidelines set forth by the World Meteorological Organization WMO-No. 1086. For other agencies, departments and entities, they will be guided by the ICT Policy unless otherwise stated.

10.6. Work Related Issues on Social Media:

When you discuss the NSWMA on work-related matters on the internet, you must identify yourself with your name and, when relevant, your role at the NSWMA. The Public Relations Office of the NSWMA are the organisations designated official spokesperson for the NSWMA or its brands, so if you are not one of them you must make clear that you are speaking for yourself and not for the NSWMA . You are requested to write a disclaimer stating "The postings on this site are my own and do not necessarily represent the position, strategy or opinions of the NSWMA and its departments". Please always write in the first person and don't use The NSWMA email address for private communications. And please consider that even anonymous postings on Wikipedia can be traced back to the NSWMA.

Do not comment on work-related legal matters unless you are an official spokesperson which was designated by the organisation, and have the legal approval by the NSWMA.

10.7. Users Responsibility on Social Media:

You are personally responsible for the content you publish on blogs, wikis or any other form of user-generated media and will be held accountable.

Respect your audience. Don't use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the NSWMA work environment. You should also show proper consideration for others privacy and for topics that may be considered objectionable or inflammatory (like religion or politics).

Don't cite or reference clients, the NSWMA officials or suppliers without their approval. When you do make a reference, where possible, link back to the source.

10.8. Designated Hours for Social Media use via the NSWMA network:

The use of social media has been officially designated as being between the hours of 12pm and 2pm. During this time, employees can access various social media sites and pages. Some acceptable and unacceptable behaviour for social media usage has been noted in **Tables 1 and 2**:

10.9. The NSWMA Acceptable Behaviour for Social Media Usage:

Table 1: Acceptable Behaviour for Social Media Usage

Be polite and respectful.	Post only appropriate and respectful content
Be honest and accurate when posting information related to the NSWMA and its staff.	No discrimination will be tolerated by the NSWMA.
Pay careful attention when providing personal information online.	Manage your self-identity and relationships.
No cyber bullying	No inappropriate pictures and comments.
Keep it professional	No online shouting (typing words in capital letters)

10.10. Unacceptable Behaviour for Social Media Usage:

Table 2: Unacceptable Behaviour for Social Media Usage

Posting negative, inappropriate, or downright inflammatory content (which may include but are not limited to, discriminatory remarks, harassment, threats of violence, unlawful conduct, for example).	Spending too much time on the social media rather than attending to the NSWMA's business.
Posting or sharing inappropriate photos and jokes.	Clicking on suspicious links and downloading inappropriate files or viruses.

Making references to drug use.	Cyber bullying
Bad mouthing employers.	Overly sharing publicly on personal or work topics especially as it relates to information about the NSWMA.
Coarse language/profanity	Posting explicit messages on one's profiles
Becoming over-friendly with work associates.	Searching or viewing a fellow co-worker's social media pages and posting inappropriate content on the page without permission.

Intentionally Left Blank

11. Account Termination

11.1 Statement of this Policy

This policy covers the disposition of email and other files stored on a NSWMA owned computer or assigned space on the NSWMA's network when an individual's employment is terminated. The NSWMA does not normally review the content of an employee's electronic communication, but these files are stored on NSWMA's computer systems and the NSWMA reserves the right to retain and access them as part of its responsibility for maintaining the NSWMA's technology infrastructure or when deemed necessary for business reasons. It is important, therefore, that when an individual leaves the employ of the NSWMA the following procedures are followed to ensure that all necessary files are transferred from these individual to the appropriate person in the NSWMA. The "appropriate person" will be identified by the departing individual's supervisor.

It is also imperative that the employee return all Mobile Devices, Computer Systems and any computer related infrastructure to the NSWMA unless there is a programme is in place to dispose of the NSWMA's assets as per direction of the Permanent Secretary (e.g mobile phone resale programme).

11.2 Scope Policy Statement

The policy is being developed to maintain the organisations infrastructure once an employee leaves and organisation and the following procedures are followed to ensure that all necessary files are transferred from these individual spaces to the appropriate person in the NSWMA. The "appropriate person" will be identified by the departing individual's supervisor.
Definition

What is Voluntary Termination?

A "voluntary termination" is characterized by mutual agreement between the employee and his/her supervisor or manager about the terms and timing of the departure, and by a determination by the supervisor/manager that he/she can work cooperatively with the departing employee to follow these procedures. It is the responsibility of the supervisor/manager to make this determination.

- **What is Involuntary Termination?**
  "Involuntary termination" usually involves little or no notice on the part of the employee and/or the supervisor/manager, under circumstances that warrant prudent measures to protect the business interests of the NSWMA.

8.2 Introduction:

This policy covers the disposition of email and other files stored on an individual's assigned computer or assigned mobile phone on the NSWMA's network when a staff member's employment with NSWMA is terminated. The NSWMA does not normally review the content of an employee's electronic communication, but these files are stored on the NSWMA's computer systems and the NSWMA reserves the right to retain and access them as part of its responsibility for maintaining the NSWMA's technology infrastructure or when deemed necessary for business reasons. It is important, therefore, that when a faculty member leaves the employment of the NSWMA, the following procedures are followed to ensure that all necessary files are transferred from the individual's spaces to the appropriate person in the NSWMA and/or provided to the staff member on a removable storage medium.

The "appropriate person" will be identified by the ICT Director or the Permanent Secretary and his designate.

11. 5 Account Termination for Staff No Longer working with the NSWMA

11.5.1 Voluntary Termination

In all voluntary termination cases, the following procedures shall apply:

1. Upon notice of termination, the staff member's Head of Department (HOD) or the Supervisor should work with the departing employee to arrange for the preservation of all business-related files both from the employee's network space and email box as well as to determine the disposition of files of a personal nature and/or related to the staff member's.
2. It is the responsibility of the HOD or the supervisor must submit to ICT Department any requests that relate to the transfer of email or other access permissions that need to be migrated from the departing staff member's to a different individual in the department, even if this is on a temporary basis.
3. It is the responsibility of the departing staff member to delete or transfer all files and email messages that are of a personal nature and/or related to her/his work. These may be transferred to a CD or flash storage drive.
4. The HOD or supervisor may request assistance from ICT Department in this process.
5. The HOD will include an item on its "staff member's exit" checklist to ensure that the above steps have been completed.
6. The HOD may decide whether files are to be transferred to a designated location on the network, such as a shared departmental space, for example, or transferred to a CD or flash storage drive.
7. Sixty (60) days after the account is disabled, the account will be deleted along with all related home directories and mailboxes unless the staff member has submitted a specific request to ICT or HRM for an extension. Any such request must clearly indicate the specific length of the extension being requested and the final date of account termination that is being requested.

8. In terms of email the staff member may opt to have a message put in place that goes to future senders of messages to his/her@xx.gov.jm email address indicating that the person is no longer employed to the NSWMA's and indicating to whom messages should be sent if the message pertains to NSWMA's business. This message will be in place for a maximum of 45 days.
9. The overall goal of these procedures is to disable the accounts of the departed staff member as soon as they are no longer actively being used. The extension of privileges will only apply to the faculty members email account. All other access will be deactivated upon termination of employment.

11.5.1.2 Involuntary Termination

In all cases of involuntary termination, the following procedures shall apply:

1. As part of the termination process, the Supervisor or the HOD should arrange with the designated staff person in ICT Department to secure all files both from the staff member's network space and email box.
2. It is the responsibility of the HOD to inform the ICT Department in advance of any involuntary termination so that appropriate arrangements may be made for the transfer of files and the timely closing of the account of the person to be terminated.
3. If so desired, ICT team will arrange to transfer all files and email messages of the terminated faculty member as part of the process of closing the

account. These may be transferred to a designated network space, CD or flash storage drive.

4. The Director ICT shall make certain that the designated person in ICT department is involved in the involuntary termination process at the appropriate time.
5. The Director ICT or System Administrator may decide whether files are to be transferred to a designated location on the network, such as a shared departmental space, for example, or transferred to a CD or flash storage drive. At the discretion of HOD, a copy of some or all of these files may be given to the terminated employee.
6. Sixty (60) days after the account is disabled, the account will be deleted along with all related home directories and mailboxes. The overall goal is to disable the account of the terminated staff immediately upon termination. This includes portal accounts, as well as facility and service access privilege

11.6 Account Termination in the Event of the Death of a NSWMA Employee

This policy covers the disposition of email and other files stored on an individual's NSWMA-owned computer and/or assigned space in the organisation in the event of the death of an employee. The NSWMA does not normally review the content of an employee's electronic communication, but these files are stored on NSWMA computer systems and the NSWMA reserves the right to retain and access them as part of its responsibility for maintaining the NSWMA's technology infrastructure or when deemed necessary for business reasons. It is important, therefore, that in the event of the death of a NSWMA employee, the following procedures are followed to ensure that all necessary files are transferred from these individual spaces to the appropriate person in the NSWMA. The "appropriate person" will be identified by the departing individual's supervisor in the case of staff and the individuals HOD in the case of a staff member.

11.7 Death of an Employee

In the event of the death of a staff member while in the employ of the NSWMA, the following procedures shall apply:

1. Upon notice of the death, an individual's supervisor should work with ICTS to arrange for the preservation of all business-related files both from the employee's network space and email box.
2. It is the responsibility of the HOD to submit to ICT Department any requests that relate to the transfer of email or other processes that need to be migrated from the departing employee to a different individual in the department, even if this is on a temporary basis.
3. Email messages and files may not be transferred to family members or other non-employees of the NSWMA for reasons of data privacy and security policies.
4. The HOD may decide whether files are to be transferred to a designated location on the network, such as a shared departmental space, for example, or transferred to a CD or flash storage drive.
5. Sixty (60) days after the account is disabled, the account will be deleted along with all related home directories and mailboxes.
6. In terms of email the HOD may opt to have a message put in place that goes to future senders of messages to the deceased employee's xx@megjc.gov.jm email address. The person's supervisor may wish to work with communications to craft such a message, but in the very least the message should indicate to whom messages should be sent if the message pertains to NSWMA business. This process would bounce the original

message back to the sender along with the new NSWMA contact information. This message will be in place for a maximum of 45 days. The forwarding of NSWMA email outside of the NSWMA will not be put place as a matter of data security and privacy policies.

7. The overall goal of these procedures is to disable the accounts of persons no longer in the employ of the NSWMA within 24 hours of his/her last day of work. This includes domain and intranet accounts, as well as any other service access privileges.

Intentionally Left Blank

12. Cellular/Smart Phone Policy Statement

12.1. Statement of Policy:

The Cellular/Smart Phone (hereinafter referred to as CS Policy) establishes guidelines for procurement, possession, and appropriate use of NSWMA-owned mobile devices. It also defines guidelines for the reimbursement of personal cellular calls and services by the employee to the NSWMA. The CS Policy is designed to reduce unnecessary cell phone costs to the NSWMA and to avoid violation of new world standards regarding cellular phone use and increase productivity by providing access to mobile solutions.

12.2 Scope of This Policy:

CS Policy is being established as guidance to employees, who by the nature of their work, have been approved to be issued with mobile devices. The Directors of Administration and ICT will determine the type of service equipment and the type of services necessary to fulfil specific NSWMA responsibilities.

12.3 Definitions:

- Cellular telephone, sometimes called mobile telephone, is a type of short-wave analog or digital telecommunication in which a subscriber has a wireless connection from a mobile phone to a relatively nearby transmitter. The transmitter's span of coverage is called a cell. As the cellular telephone user moves from one cell or area of coverage to another, the telephone is effectively passed on to the local cell transmitter 4.

12.4 Introduction

NSWMA employees are strongly discouraged from using a NSWMA - provided cell/smart phone for personal business. NSWMA employees are also discouraged from conducting NSWMA business on any cell/smart phone while operating a motor vehicle. Employees are encouraged to use "hands-free" phones in limited situations and not for prolonged conversations. Cell/Smart phone use while driving should only occur in an emergency situation.

The CS Policy applies to mobile devices including all cell/smart phone contracts, entered into by the NSWMA, effective as of the date of this policy. Department Heads may establish mobile device use policies that are more but not less restrictive than this policy.

Note: All assignments and changing of device, data plan and talk plan are to be approved by the Permanent Secretary within the NSWMA.

12.5 Entities/Personnel Affected by the Policy

4 http://searchmobilecomputing.techtarget.com/definition/cellular-telephone

The persons who are affected by the CS Policy are all users assigned NSWMA-owned cell phones. The NSWMA personnel who are responsible for distributing cellular/smart phones and tablets are listed below.

- Director of Administration
- Cellular Network Representative
- System Administrator

12.6 Roles and Responsibilities

- **Permanent Secretary:** Approval authority for all cellular phone purchases and contracts when the NSWMA is the official billing entity. He/she will also have the authority to approve limits and plans ascribe to each user.

- **Director of Administration:** Review monthly cell phone bills received from Telecommunications section. Budget all funds to pay monthly cellular bill. Notify employees who have exceeded monthly service plan costs or exceeded incidental personal use threshold.

- **Cellular Network Representative:** Provides technical and business support for the NSWMA of Water, Land, Environment and Climate Change as requested.

- **System Administrator:** Configures and provides technical assistance with email problems on tablets or NSWMA smart phones that the service is accessible.

- **Auditors:** Periodically review CS Policy and procedures, and perform spot checks for adherence.

Usage Policy

Details of the Use of Government Mobile Telephones and Closed User Group (CUG) Systems. (Reference: Circular No. 8/2009 File No. 451/016)

13. Change process (How to make changes to this document)

1. **Start a new document by modifying the name of the current version (Example: "Quality Documents Template_v1.0" should be changed to "Quality Documents Template_v1.1" for content changes OR "Quality Documents Template_v2.0" for Template/Format changes by using the** "Save As" **function.**
    a. **Content changes are changes that have to do with information, for example a change of the way a process(es) is done within the document**
    b. **Template changes are changes having to do with the overall format of the document**
2. **Update the internal document with the version information, using the table set out on the Title Page with information such as Author, version number, etc…**
3. **Update the document content as necessary**
4. **Submit to the IT Manager for Verification/Vetting**
5. **Submit to The IT Director for Approval to publish/implement, after which the "Approved By" and "Implementation Date" attributes are to be updated.**
6. **Publish the document by saving it as a PDF document using the naming convention - <<document_title>>_v<<version_number>>**
7. **Apply any relevant policy restrictions such as** no print, password**, etc…**