ICT Transformation Programme

PSG Manual

ICT Policies, Standards & Guidelines

Prepared by

The Office of the Chief Information Officer - Jamaica

Government of Jamaica

February 2018

DOCUMENT

Date of issue/Update	Created: <04-Dec-2017 > Last reviewed and/or updated: 26-Feb-2018	Version	<1.2>
Status	**Production Release**		
Owner	The Office of the Chief Information Officer - Jamaica		
Approved by:	Chief Information Officer	<dd month year >	
ICT Council sign off needed?	Yes or No	<dd month year >	

REVISION HISTORY

Version	Issue Date	Revision Description

Letter of Transmittal

Feb 25, 2018

TO: the Permanent Secretary, Ministry of Science, Energy & Technology

"Time for just strategies is over, time for action is now" because "A strategy without implementation is just hallucination" !

I am pleased to submit this Draft Policies, Standards and Guidelines (PSG) report which is a consolidation of the first 9 PSGs as stipulated in the IDB Funding. Needless to say, there are many other PSGs that are being pursued as operational tools that would be used by the **ICT Authority** in support of the ICT Governance Framework approved by Cabinet.

In keeping with the "Made in Jamaica" theme, the help of many executives, management and staff in the GoJ and particularly from eGovJA was sought to deliver this report over the course of the past couple of years. In particular, I wish to thank members of the Project Portfolio Management Committee of the ICT Council (PPMC) who created a Task Force that specifically deals with these PSGs and continue to do so on an ongoing basis. To our Hon. Minister of MSET and to yourself, Permanent Secretary and to all contributors we wish to convey our sincere thanks and gratitude for the opportunity to compile these PSGs that we believe will be the reference manual that our MIS Officers and staff will be using in their everyday work.

We are certain that there will be a lot more consultation and many questions and enquiries on how this document and its future versions will be used and the ICT Authority will be challenged to make this PSG document the right reference on many of the operating policies, standards and guidelines as practiced in the GOJ.

We invite your consideration of this document as another partial deliverable of our GoJ ICT Transformation Process.

Respectfully submitted

Dr Louis Shallal, P.Eng., Ph.D

CIO Jamaica

This Page Intentionally Left Blank

Contents

This Page Intentionally Left Blank

1. Preface

This Manual encapsulates the Information & Communications Technology Policies, Standards, and Guidelines (PSGs) as compiled by the Office of the CIO with ongoing efforts of this Office and the work of the PSG SubCommittee of the Programme Portfolio Management Committee (PPMC).

This document is the result of a process delineated as follows:

1. Conceptualization of the PSGs collection effort; this was effected as a component of the ICT Transformation Process during the consultations which we conducted with MIS Officers and the GoJ ICT organisation.
2. From that conceptualization we confirmed from the MIS Officers the need, by asking whether these policies and guidelines were necessary and received affirmative responses from them.
3. A survey was conducted of available PSGs which MDAs currently had in use; we compiled these from all the MDAs, compared, consolidated addressing overlaps (as many MDAs had developed a number of PSGs independently of each other), and synthesized where possible, in order to arrive at a set for the GoJ which addressed current practices and usage within the MDAs, bringing these together into one collection.
4. Next was the circulation across the MDAs of the draft list developed from the previous steps, requesting input and comments. These were presented at our bi-monthly MIS Officers Forum, where we informed the ICT community of what we were doing; responses were received from the MIS Officers as to how necessary and effective these would be. The collected documents were added to by the adoption and 'Jamaicanisation' of some PSGs from an external jurisdiction. We hereby acknowledge with gratitude the use of these external sources. Currently these documents populate a repository on Alfresco.
5. The CIO will be informing the heads of the MDAs through a letter to the PS Board so that they can, in turn, advise MIS Officers of the availability of these, and to convey that the Office of the CIO would be happy to assist MDAs with implementation and queries on these PSGs.

The PSG Subcommittee of the PPMC has recognised the need to put tools and mechanisms in place to manage the implementation of policies, standards, and guidelines, covering matters such as monitoring and compliance, help desk functionality, and implementation assistance. Terms Of Reference for the sub-committee have been produced, and a Policy Implementation Process Flow has been documented. It is our opinion that this document will become one of the main source documents that the **New ICT Authority** will use in an effort to harmonize the various processes in the GoJ.

It should be noted that unless otherwise specified, and notwithstanding that the new ICT Authority is not yet established, all references to authority and responsibility for ICT has been assumed to apply to the ICT Authority.

2. Introduction

This is a living document, sectioned separately into Policies, Standards and Guidelines; the initial release contains the first (1st) nine (9) PSGs to be released for production use. New editions will be released as additional documents from the collected pool are moved to production status.

The PSGs in the collection were authored by different contributors with different styles. The PSG Team has applied significant effort into ensuring consistency in presentation of these; although this has not always been possible, the fundamental structure has been adhered to, and it is acknowledged that refinements will take place over time.

All References to IT in the document should be and is equally applicable to ICT. The reference to IT was done for the sake of simplicity and to a certain extent in conformity with international references. However, where there is a specific need to refer to an already established name such as ICT Governance Framework, the full ICT letters are used.

The PSGs covered in this Manual are listed here:

- **Policies**
  - *Policy Framework for Information and Communications Technology*
  - *Policy On Management of Information Technology*
  - *Policy On Acceptable Network and Device Use*
- **Standards**
  - *Standard for Email Management*
  - *Standard for Electronic Documents and Records Management Solutions (EDRMS)*
  - *Standard for Operational Security*
- **Guidelines**
  - *Guidelines for Secure Connections Across GoJ Web Sites and Services*
  - *Guidelines for Official Use of Social Media*
  - *Guidelines for GoJ Cloud Computing*

3. Policies

- Policy Framework for Information and Communications Technology
- Policy On Management of Information Technology
- Policy On Acceptable Network and Device Use

Policy Framework for Information Technology

1. Application

1.1. This policy applies to all users of information technology solutions within government owned companies, public bodies and the Ministries, Departments and Agencies (MDAs) of the Government of Jamaica, and must be adhered to by all MDAs unless excluded by specific acts, or regulations**.**

2. Context

2.1. The established GOJ **ICT Governance Framework** has brought into focus the need for governance and management of a logical structure that is established with defined processes to organize IT policy documentation and the planning, development, approval, implementation and monitoring of the IT policies. This document specifies the Policy Governance and Management Framework that defines the interaction among various stakeholders to create IT Policies that will be implemented by government owned companies, public bodies and the MDAs of the Government of Jamaica.

3. Definitions

3.1. Definitions to be used (Terms, Acronyms, etc.) in interpretation of this policy are provided in Section **9. Glossary Of Terms**.

4. Policy Statement

4.1. Objective

The objective of this policy is to establish the relevant IT Policy Governance and Management Framework within which the information technology Policies, Standards, Guidelines, and Best Practices for the GoJ are developed, approved, implemented and reviewed in order to ensure relevant and adequate support to the Government's efforts to secure its IT assets and promote the most efficient use of its technology resources. These policies will aid in the mitigation of risks associated with the use of ICT resources in the business of Government and its interaction with citizenry and the private sector.

4.2. Expected Results

The expected results of this policy are:

- a better understanding on the part of all key stakeholders of their roles and responsibilities with respect to the management of IT in the government;
- strengthened management of IT across the government and better decision-making at all levels, thus ensuring that IT supports program delivery and provides value for money;
- increased use of common or shared IT assets and services by MDAs to ensure efficiency gains; and
- responsive services enabled by IT.

5. Policy Requirements

5.1. Permanent Secretaries

Permanent Secretaries are responsible for ensuring that:

5.1.1. common or shared IT assets and services are used in ministries to avoid duplication, when such assets and services are available and appropriate;

5.1.2. GoJ ICT governance structures are adhered to;

5.1.3. performance related to the MDA management of IT is measured on an ongoing basis;

5.1.4. GoJ departments provide ICT Council / PPMC with information concerning their activities in relation to this policy.

5.2. Monitoring and Reporting Requirements

Permanent Secretaries / Heads Of Agencies

5.2.1. These executives are responsible for monitoring adherence to this policy within their organizations, and for ensuring that appropriate remedial action is taken to address any deficiencies identified.

Government-wide

5.2.2. The ICT Council will review this policy, its associated directives and standards, and their effectiveness at the five-year mark of implementation of the policy (or earlier for certain directives and standards). When substantiated by risk analysis, the ICT Council will also ensure an evaluation is conducted. Compliance to GoJ ICT Policies will be verified through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and inspection.

6. Consequences

6.1. Consequences of non-compliance are in accordance with existing practices within the GoJ and can include informal follow-ups and requests from ICT Council, external audits, and formal direction on corrective measures.

7. Management Roles and Responsibilities

7.1. The ICT Authority is responsible for the management and operation of the common and shared IT services in consultation with MSET and the ICT Council.

7.2. The ICT Council is responsible for establishing the overall government-wide strategic directions for IT; identifying areas that offer significant government-wide benefits or are of importance to the government; and leading initiatives to achieve government-wide solutions

and the implementation of government-wide directions with the appropriate common service or shared service organizations that are of importance to the government.

7.3. All Departments within government owned companies, public bodies and the MDAs of GOJ that use information technology (IT) must:

- Adhere to the IT Policies issued by the ICT Authority
- Develop and implement, when appropriate, additional IT Policies Standards and Guidelines (PSGs) specific to their operating units.
- Promote IT Policy adherence.
- Comply with the requirements of this Policy Governance and Management Framework.
- Inform the Office of the CIO / ICT Authority if there are any problems with a policy or if business interactions are inconsistent with the defined policies.
- Provide all employees with instruction and/or documented Policies, Standards and Guidelines (PSGs) that relate to their job descriptions.
- Provide an annual "refresher" for current employees highlighting the changes made to PSGs or problem areas during the previous year.
- Facilitate training and the dissemination of information on PSGs.

8. Enquiries

8.1. The ICT Council is responsible for the policy instruments supporting this policy framework; please direct any enquiries to:

Chief Information Officer

Office of the CIO

(876) 929-8990 - 9
(876) 960-1623
cio@mset.gov.jm

9. Glossary Of Terms

Client

The intended recipient of a service. Clients may be external (citizens, businesses, non-Jamaicans, or organizations, e.g., non-profit) or internal to government (MDAs).

Common service

A service that is provided by a common service organization.

Information technology

Includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation and implementation of information and communication systems and applications to meet business requirements.

Service

A means, administered by a program, of producing a final valued output (i.e. service output) to address one or more target group needs.

Shared service

A service that is shared by more than one client.

Policy on Management of Information Technology

1. Application

1.1. This policy applies to all MDAs unless excluded by specific acts, or regulations**.**

2. Context

2.1. Information technology (IT) plays an important role in government operations. It is also a key enabler in transforming the business of government. Information technology is an essential component of the government's strategy to address challenges of increasing productivity and enhancing services to the public for the benefit of citizens, businesses, taxpayers and employees.

2.2. Permanent Secretaries and Heads of Agencies are responsible for the effective management of IT within MDAs, including the implementation of ITspending decisions and ensuring adherence to specified practices for appropriate ongoing measurement of IT performance.

3. Definitions

3.1. Definitions to be used (Terms, Acronyms, etc.) in interpretation of this policy are provided in Section **9. Glossary of Terms**.

4. Policy Statement

4.1. Objective

The objective of this policy is to achieve efficient and effective use of information technology to support government priorities and program delivery, to increase productivity, and to enhance services to the public.

4.2. Expected Results

The expected results of this policy are:

- a better understanding on the part of all key stakeholders of their roles and responsibilities with respect to the management of IT in the government;
- strengthened management of IT across the government and better decision-making at all levels, thus ensuring that IT supports program delivery and provides value for money;
- increased use of common or shared IT assets and services by MDAs to ensure efficiency gains; and
- responsive services enabled by IT.

5. Policy Requirements

5.1. Permanent Secretaries

Permanent Secretaries are responsible for ensuring that:

5.1.1. common or shared IT assets and services are used in ministries to avoid duplication, when such assets and services are available and appropriate;

5.1.2. GoJ ICT governance structures are adhered to;

5.1.3. performance related to the MDA management of IT is measured on an ongoing basis;

5.1.4. GoJ departments provide ICT Council / PPMC with information concerning their activities in relation to this policy.

5.2. Monitoring and Reporting Requirements

Permanent Secretaries / Heads of Agencies

5.2.1. These executives are responsible for monitoring adherence to this policy within their organizations, and for ensuring that appropriate remedial action is taken to address any deficiencies identified.

Government-wide

5.2.2. The ICT Council will review this policy, its associated directives and standards, and their effectiveness at the five-year mark of implementation of the policy (or earlier for certain directives and standards). When substantiated by risk analysis, the ICT Council will also ensure an evaluation is conducted..

6. Consequences

6.1. Consequences of non-compliance are in accordance with existing practices within the GoJ and can include informal follow-ups and requests from ICT Council, external audits, and formal direction on corrective measures.

7. Management Roles and Responsibilities

7.1. The ICT Authority is responsible for the management and operation of the common and shared IT services in consultation with MSET and the ICT Council.

7.2. The ICT Council is responsible for establishing the overall government-wide strategic directions for IT; identifying areas that offer significant government-wide benefits or are of importance to the government; and leading initiatives to achieve government-wide solutions and the implementation of government-wide directions with the appropriate common service or shared service organizations that are of importance to the government.

8. Enquiries

8.1. The ICT Council is responsible for the policy instruments supporting this policy framework; please direct any enquiries to:

Chief Information Officer

Office of the CIO

(876) 929-8990 - 9
(876) 960-1623
cio@mset.gov.jm

9. Glossary of Terms

Client

The intended recipient of a service. Clients may be external (citizens, businesses, non-Jamaicans, or organizations, e.g., non-profit) or internal to government (MDAs).

Common service

A service that is provided by a common service organization.

Information technology

Includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation and implementation of information and communication systems and applications to meet business requirements.

Service

A means, administered by a program, of producing a final valued output (i.e. service output) to address one or more target group needs.

Shared service

A service that is shared by more than one client.

Policy on Acceptable Network and Device Use

1. Application

1.1. This policy applies to the use of Government of Jamaica electronic networks by staff for conducting government business and professional use, regardless of location of access or device used, to perform activities as a part of their official duties, for career development and other professional activities, and for limited personal use that is conducted on personal time that is not for financial gain, does not incur any additional costs for the MDA, and that does not interfere with the conduct of government business.

2. Context

2.1. The Government of Jamaica recognizes that open access to Government of Jamaica electronic networks and devices, including the Internet, is essential to transforming the way public servants work and serve Jamaicans. Open access to the Internet including Government of Jamaica and external Web 2.0 tools and services will enhance productivity, communication and collaboration, and encourage the sharing of knowledge and expertise to support innovation. All use of Government of Jamaica electronic networks and devices must be in compliance with all values and ethics codes for the public sector and all other related policies and ministerial codes of conduct and policies. Use of Government of Jamaica electronic networks and devices must not give rise to a real, potential or apparent conflict of interest or in any way undermine the integrity of the MDA.

2.2. Permanent Secretaries and Heads of Agencies are responsible for the effective management of IT within MDAs, including the implementation of ITspending decisions and ensuring adherence to specified practices for appropriate ongoing measurement of IT performance.

2.3. This policy is issued by the ICT Council.

3. Definitions

3.1. Definitions to be used (Terms, Acronyms, etc.) in interpretation of this policy are provided in Section **11. Glossary of Terms**.

4. Policy Statement

4.1. Objective

The objective of this policy is to ensure acceptable and efficient use of Government of Jamaica electronic networks and devices to support enhanced communication and collaboration thereby improving productivity, and program and service delivery to individuals and businesses.

4.2. Expected Results

The expected results of this policy are:

- Authorized individuals use of Government of Jamaica electronic networks and devices in an acceptable manner; and
- Provision to authorized individuals of open access to the Internet including Government of Jamaica and external Web 2.0 tools and services, in accordance with the GoJ policies and standards on security.

5. Policy Requirements

5.1. Permanent Secretaries and Heads Of Agencies are responsible for ensuring that:

5.1.1. Effective management and monitoring practices for the acceptable use of Government of Jamaica electronic networks and devices are implemented.

5.1.2. Authorized individuals are informed of the following:

- Expectations for acceptable use of Government of Jamaica electronic networks and devices per Appendices B and C;
- Electronic network monitoring practices being applied by their own MDA; and
- Consequences for unacceptable use of such networks and devices.

5.1.3. Authorized individuals have open access to the Internet including Government of Jamaica and external Web 2.0 tools and services that enhance productivity, communication and collaboration.

5.1.4. Learning opportunities regarding the acceptable use of Government of Jamaica electronic networks and devices and Government of Jamaica and external Web 2.0 tools and services are provided to authorized individuals.

6. Monitoring and Reporting Requirements

6.1. Permanent Secretaries / Heads Of Agencies are responsible for:

a) monitoring adherence to this policy within their organizations, and for ensuring that appropriate remedial action is taken to address any deficiencies identified.

Government-wide

6.2. The ICT Council is responsible for:

a) oversight and monitoring of the compliance with this policy by permanent secretaries through an annual confirmation that policy requirements are being met, leveraging existing reporting mechanisms where applicable;
b) recommending that corrective action be taken when a MDA has not complied with the requirements of this policy; and
c) establishing a framework for the review of this policy and ensuring that a review is initiated within five years of the effective date of this policy.

7. Consequences

7.1. Consequences of non-compliance are in accordance with existing practices within the GoJ and can include informal follow-ups and requests from ICT Council, external audits, and formal direction on corrective measures.

8. Management Roles and Responsibilities

8.1. The ICT Authority is responsible for the management and operation of the common and shared IT services in consultation with MSET and the ICT Council.

8.2. The ICT Council is responsible for establishing the overall government-wide strategic directions for IT; identifying areas that offer significant government-wide benefits or are of importance to the government; and leading initiatives to achieve government-wide solutions and the implementation of government-wide directions with the appropriate common service or shared service organizations that are of importance to the government.

9. References

- Access to Information Act
- Data Protection Act (under development)
- Standard for Operational Security
- Policy Framework for Information and Technology
- Policy on Acceptable Network and Device Use
- Standard for Electronic Document and Records Management Solutions
- Standard for Email Management
- Guidelines for Secure Connections Across GoJ Web Sites and Services
- Guidelines for Official Use of Social Media
- Guidelines for GoJ Cloud Computing

10. Enquiries

10.1. The ICT Council is responsible for the policy instruments supporting this policy framework; please direct any enquiries to:

Chief Information Officer

Office of the CIO

(876) 929-8990 - 9
(876) 960-1623
cio@mset.gov.jm

11. Glossary Of Terms

Acceptable use

Permitted use of Government of Jamaica electronic networks and devices by authorized individuals.

Access

Gaining entry to an electronic network that the government has provided to Government of Jamaica authorized individuals. Access to such electronic networks may be from inside or outside government premises. Access may support telework and remote access situations, or situations where authorized individuals are using electronic networks provided by the government on their own time for limited personal use.

Authorized individuals

Individuals working with the Government of Jamaica, including employees of the government as well as other persons who have been authorized to access Government of Jamaica electronic networks and devices.

Electronic network

Groups of computers and computer systems that can communicate with each other, including without limitation, the Internet, Government of Jamaica electronic data networks, voice and video network infrastructure, and public and private networks external to a MDA. The network includes both wired and wireless components.

External networks

Networks reached from the Government of Jamaica network, to which authorized individuals are granted access. They include permissible sites across the public Internet and via the World Wide Web, including services provided by parties such as collaborative software.

Internet

A global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve users worldwide.

Learning opportunities

Diverse learning methods or tools, formal or informal, to generate awareness or acquire knowledge about the acceptable use of Government of Jamaica electronic networks and devices and Government of Jamaica and external Web tools and services. These approaches can include, but are not limited to, information or orientation sessions, YouTube video, information provided on ministry's intranet sites, manager debriefs, account sign-on notifications and electronic newsletters.

Monitoring practices

Use of a software system that monitors an electronic network for slow or failing components, and notifies the network administrator in cases of outages, and that can monitor the network activity of specific individuals for which there is suspicion of unacceptable network usage. Recording and analysis of the use of electronic networks are used for operational purposes and for assessing compliance with government policy.

Open access

Refers to the provision of Internet access, to authorized individuals via Government of Jamaica electronic networks and devices that, from the perspective of firewall settings, is substantively equivalent irrespective of ministry or access medium. Internet sites that enhance productivity, communication and collaboration are not blocked with the exception of those that present a legitimate IT security threat and where content substantively falls into the category of unacceptable use.

Unacceptable use

Any activity that violates any policy instruments or other published requirements, including, but not limited to, activity or behavior that:

- May give rise to criminal offences;
- Violates statutes;
- Impacts negatively on the performance of Government of Jamaica electronic networks and devices;
- Impedes GoJ operations or the delivery of services; and
- Could be deemed to reasonably result in civil lawsuits.
-

User devices

Physical devices found or brought into the work environment that are used by authorized individuals to access Government of Jamaica electronic networks and databases. The physical devices can include, but are not limited to, the following: desktop workstations, laptops, notebooks, tablets, smartphones, cellphones, peripherals such as printers and scanners, memory devices such as USB flash drives, CD drives and DVD drives, webcams and any other computer hardware used to obtain, store or send information.

Web 2.0

Includes Internet-based tools and services that allow for participatory multi-way information sharing, dialogue, syndication, and user-generated content. This can include social media and collaborative technologies.

12. Appendix

Appendix A. Examples of Acceptable Use (non-exhaustive list)

Open access to the Internet, including Government of Jamaica and external Web 2.0 tools and services, can assist authorized individuals to conduct the business of government more efficiently and effectively. The acceptable use of Government of Jamaica electronic networks, devices and internal and external Web 2.0 tools and services will support the transformation of how public servants perform their work duties, enhance collaboration and networking with their peers, augment professional development opportunities and enable limited and reasonable personal use during work hours.

As well, informing users of expected behaviours when using networks, devices and Government of Jamaica and external Web 2.0 tools and services will help them to protect against potential confidentiality or privacy issues.

The following are non-exhaustive lists of examples of acceptable use of internal and external Web 2.0 tools and services that could be conducted via Government of Jamaica electronic networks and devices.

Work-related and Professional Development Activities

1. Conduct consultations within the government via internal wikis and forums to support the development of policies and programs;
2. Share knowledge and information intra- or inter-ministerial to support planning and decision-making or facilitate project collaboration;
3. Perform research through accessing online reports, presentations, and data-sets;
4. Watch online broadcasts of work-related content, such as a parliamentary committee meeting;

5. Remain up-to-date with official announcements published on social media platforms by ministries and agencies, local government, or international jurisdictions or organizations;
6. Document corporate knowledge on Government of Jamaica wikis to facilitate employee orientation and knowledge transfer;
7. Participate in a video or audio conference with colleagues or clients from other organizations or jurisdictions through tools such as Skype or Google Hangouts;
8. Develop and share code repositories in collaboration with ministries, other jurisdictions and private sector organizations via code sharing tools such as GitHub;
9. Leverage expertise from across government by creating or participating in online communities of interest on topics of shared professional interest;
10. Access or share unclassified information through cloud-based tools such as SlideShare;
11. Collaborate on joint initiatives and projects, via open discussions or closed groups as appropriate, with other ministries and levels of government through the use of wikis, professional networking applications, internal tools such as GCDocs or external cloud-based tools such as Google Docs;
12. Maintain an up-to-date profile on professional networking sites such as LinkedIn;
13. Follow thought leaders and government officials on blogs or micro-blogs such as Twitter;
14. Tweet, re-tweet or share links to professional activities and events, or interesting and relevant articles;
15. Read, contribute to, or edit articles in work-related wikis, online forums or discussion groups;
16. Discuss professional issues or participate in professional associations via online forums or social networking sites;
17. Participate in online professional training activities (e.g. webcasts, online learning products via CSPS, podcasts);
18. Find a colleague or client's contact information or directions to a meeting;
19. Make arrangements for work-related travel, including booking tickets and searching for information about accommodations via Government of Jamaica or third-party travel review services; and
20. Complete an online job application or participate in an online interview.

Note: Open access in departments will occur incrementally as ministerial bandwidth restrictions are resolved.

Limited Personal Use

Examples of limited personal use that is conducted on personal time, that is not for financial gain, that does not incur any additional costs for the ministry, and that does not interfere with the conduct of business include:

1. Search for information online;
2. Keep up-to-date with news and current events;
3. Subscribe to Web feeds (such as RSS) ;
4. Get directions for a trip or search for addresses and contact information;
5. Make personal travel arrangements;
6. Post or read ratings/reviews of products or services or make online purchases;
7. Check the weather forecast;
8. Confirm bus schedule information;
9. Pay bills or conduct personal banking online;
10. Read / contribute to online forums, blogs, discussion groups, or personal interest wikis;
11. Update a personal blog, micro-blog, social networking page, or Web page that is for non-commercial purposes or does not otherwise constitute Unacceptable Use as per Appendix C; and
12. Visit social networking sites to connect with family and friends.

Appendix B. Examples of Unacceptable Use (non-exhaustive list)

The legal consequences of unacceptable use will be determined by the section of the law in default. The employment consequences of unacceptable use will be determined by existing policy instruments and guidance from appropriate organizational human resources or labour relations advisors. MDAs can limit the use of Government of Jamaica electronic networks and devices or impose employment consequences if the activity or behaviour:

- Is unacceptable or criminal in nature;
- Violates organizational policies and codes of conduct and other published requirements;
- Impacts negatively the performance of Government of Jamaica electronic networks and devices;
- Impedes organizational operations or the delivery of services; or

Criminal offences

The following is a non-exhaustive list of examples of criminal activity that could take place on Government of Jamaica electronic networks or devices:

1. Child pornography-Possessing, downloading or distributing any child pornography.
2. Copyright infringement-knowingly distributing infringing copies of a copyrighted work.
3. Defamation-Causing a statement to be read by others that is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person.
4. Denying right of access under the Access to Information Act: destroying, mutilating, altering, falsifying or concealing a record, or making a false record with intent to deny a right of access under the Access to Information Act.
5. Hacking and other crimes related to computer security.
6. Gaining unauthorized access to a computer system-Using someone else's password or encryption keys to engage in fraud or obtaining money, goods or services through false representations made on a computer system.
7. Trying to defeat the security features of the electronic networks.
8. Spreading viruses with intent to cause harm.
9. Destroying, altering or encrypting data without authorization and with the intent of making the data inaccessible to others who have a lawful need of access.
10. Interfering with others' lawful use of data and computers.
11. Sending electronic messages that cause harassment to people, or fear for their safety or the safety of anyone known to them.
12. Interception of private communications or electronic mail (in transit)-Unlawfully intercepting someone's private communications or unlawfully intercepting someone's electronic mail.
13. Obscenity-Distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material.
14. Various other offences-The Cybercrimes Act provides for a range of other offences that can take place in whole or in part using electronic networks. The following is a non-exhaustive list of examples of illegal (though not criminal) activity that could take place while accessing the Internet through Government of Jamaica electronic networks or devices:

    - Disclosing sensitive information without authorization.
    - Disclosing personal information-Failing to respect the privacy and dignity of every person.

- Disclosing business trade secrets-Revealing business trade secrets without authorization, other than in response to a formal request under the Access to Information Act.
- Disclosing sensitive government information-Revealing sensitive government information without authorization.
- Intellectual property infringement: infringing or otherwise using without authorization another person's intellectual property (copyright, trade-mark or patent).
- Privacy breaches-Include, but is not limited to, any of the following without authorization: reading someone else's electronic mail or other personal information, listening in on someone's private conversations or intercepting electronic mail while it is in transit, for example.
- Various other offences-The Cybercrimes Act provides for a range of other offences that can take place in whole or in part using electronic networks.

Violation of organizational policies and publications

The following is a non-exhaustive list of examples of activities that contravene policies (and may contravene comparable organizational policies):

- Causing congestion and disruption of Government of Jamaica electronic networks and systems through such means as sending chain letters and receiving list server electronic mail unrelated to a work purpose.
- Using the Government of Jamaica electronic networks for unauthorized activities as laid out in this policy and related guidance
- Using Government of Jamaica electronic networks to make public comments about government policies, except when acting as the official spokesperson.
- Representing personal opinions as those of the organization, or otherwise failing to comply with organizational procedures concerning public statements about the government's positions.
- Providing authorized individuals with access to systems, networks or applications used to process sensitive information before such personnel are properly security screened.

- Failing to revoke system access rights of personnel when they leave the organization due to the end of employment or the termination of a contract, or when they lose their reliability status or security clearance.
- Unauthorized removal or installation of hardware or software on government owned informatics devices or electronic networks.
- Furthermore, unless for valid work-related purposes, authorized individuals cannot use Government of Jamaica electronic networks or devices to access or download websites or files, or send or receive electronic mail messages or other types of communication, that fall into the following categories:
    - Documents that incite hatred against identifiable groups contained in personal messages;
    - Documents whose main focus is pornography, nudity and sexual acts.

Activity that can expose authorized individuals or the employer to tort liability

Various kinds of conduct can expose a person or an employer to civil liability. The employer's liability will be triggered when a public service employee or authorized individual performs the activity. The following is a non-exhaustive list of examples of torts from which liability may stem from activity on Government of Jamaica electronic networks or devices:

- Disclosing or collecting sensitive data-Revealing or obtaining such information without authorization. In addition to the statutory provisions mentioned above, an unauthorized disclosure or collection of personal information can result, in some circumstances, in a civil action for invasion of privacy, nuisance or trespass under common law, for breach of contract and for breach of trust or breach of confidence (e.g., if confidential commercial information is disclosed).
- Defamation-Spreading false allegations or rumors that would harm a person's reputation. In addition to criminal libel, publishing defamatory statements without a lawful defence can result in a civil action.
- Inaccurate information-Posting inaccurate information, whether negligently or intentionally. This can lead to civil lawsuits for negligent misrepresentation.

Note: The above is a non-exhaustive list of unacceptable use. Other activities could be deemed unacceptable at the discretion of a Permanent Secretary / Head of Agency.

Appendix C. Privacy

Privacy Notices

Authorized individuals must be informed of ministerial monitoring practices via a privacy notice, prior to their implementation, by communicating at a minimum, the following information:

- A statement explaining the regular monitoring practices of electronic networks-for example, operational analysis of logs indicating the Internet sites employees and other authorized individuals have visited, the files downloaded or uploaded, or the key-word searches of files on network servers or on computer storage devices of Government of Jamaica employees or other authorized individuals' computers;
- A statement that electronic networks will be monitored for work-related purposes-for example, to assess system or network performance, protect government resources or ensure compliance with government policies; and
- A statement that special monitoring may be permitted without notice in instances where illegal or other unacceptable use is suspected.

MDA Considerations for Privacy

1. While the organization is required by law to protect personal information gathered with appropriate authority for business purposes, information and technology assets are assigned to individuals for authorized use only. If users choose to store their own personal information on the network or any other equipment, it is at their own risk.
2. Whenever individuals involved in an investigation are obliged to read the content of electronic communications, they must keep the information confidential and use it only for authorized purposes.
3. Under the *Access to Information Act* , the public may request access to the Government of Jamaica's information or electronic records, as well as their own personal information, subject to applicable exemptions under those Acts. These records include electronic mail that Government of Jamaica employees or other authorized individuals have sent or received that is stored on government computers and records showing which websites Government of Jamaica employees or other authorized individuals have visited.

Appendix D. -MDA Considerations for Security (non-exhaustive list of examples)

The Government of Jamaica recognizes that cyber threats are increasing with the global reach of the Internet and the growing interconnections of government and non-government networks worldwide.

As ministries open access to their electronic networks and devices, hackers and cybercriminals have more opportunities to gain unauthorized access to sensitive government information through Government of Jamaica networks and systems. As a result, Government of Jamaica departments must be ever more vigilant in today's dynamic threat environment as malicious code can be hidden in known or trusted web sites, tools and services.

Ministries remain responsible for ensuring that they comply with the requirements established in Government of Jamaica security policy instruments

Ministries are to ensure that, based on an analysis of ministerial security needs, security measures from the following non-exhaustive list are selected, properly implemented and layered in a manner that will provide defence-in-depth and will help to protect Government of Jamaica electronic networks, devices and information:

1. Use currently supported versions of operating systems and applications (and ensure that they remain patched and up-to-date) to reduce vulnerabilities in software that can be remotely exploited;
2. Disable unnecessary features in operating systems, applications and web browsers to reduce attack surface;
3. Disable auto-run functionality on endpoints to prevent accidental code execution;
4. Enable data execution prevention in operating systems and applications to reduce the risk of memory overflow execution by malicious code;
5. Use antivirus software with up-to-date signatures and heuristic detection capabilities at the gateway and on endpoints to detect and prevent the execution of malicious code;
6. Implement host-based intrusion detection/prevention (IDP) systems to improve the ability to detect and identify anomalous behaviours;
7. Use whitelisting or blacklisting to prevent access to malicious websites, tools and web-based services from GoJ networks and devices;
8. Implement centralized logging for computer events, with regular log analysis, to improve the ability to detect and identify anomalous behaviours and to assist with incident management and forensic analysis of compromised systems;

9. Ensure that user accounts with administrative or root privileges are not used to search, browse or collaborate over the internet - these users should instead use normal user accounts with standard privileges; or a solution that will prevent the use of, or drop, administrator privileges;
10. Use network segmentation, segregation and access controls to control how devices and systems that allow users to access Internet-based web-content are allowed to interact with other high-value systems and assets; and
11. Ensure that security awareness programs include:
    a. Material notifying users that they are not permitted to post or share sensitive GoJ information (i.e. classified, protected, proprietary or otherwise restricted-distribution material) on public web sites, tools and services;
    b. Material discussing the threats and risks associated with Internet-based web-content as well as measures users can take to reduce risks;
    c. Material describing the threats and risks associated with mobile device use as well as measures users can take to reduce risks; and
    d. Regular reminders and updates to maintain awareness and to reflect the latest trends and threats.

This Page Intentionally Left Blank

13. Standards

- Standard for Email Management
- Standard for Electronic Documents and Records Management Solutions (EDRMS)
- Standard for Operational Security

This Page Intentionally Left Blank

Standard for Email Management

1. Application

1.1. This standard applies to all MDAs unless excluded by specific acts, or regulations**.**

1.2. This standard applies to all Government of Jamaica email sent and received, all Government of Jamaica instant messages sent and received, and all Government of Jamaica email services, including those classified secret and above.

1.3. As the designated ICT Authority (at this time eGovJA and the Office of the CIO, Jamaica) assumes the responsibility of administering email services for additional departments, the requirements outlined in Sections 5.1.3, 5.1.4 and 5.2.1 will apply.

2. Context

2.1. Electronic messaging can take many forms, including email in a user's account, instant messages, or email in a generic account or public folder. Consistent management of all forms of electronic messaging facilitates efficient and effective management of information resources of business value.

2.2. Electronic mail, or email, is one of the most commonly used forms of communication in the Government of Jamaica. Email is an essential tool for modern communications, which enables internal and external government services. Government employees and citizens interacting with the government use email to create, send, and receive information quickly and easily. Employees have a responsibility to manage their email and instant messages to ensure the effective and efficient use of government resources and technology.

2.3. Establishing an environment in which email and instant messages are managed consistently to meet business needs and comply with applicable laws, policies, and directives facilitates decision making, transparency, and accountability; reduces risks related to information retention and disposition; and ensures the efficient delivery of government programs and services.

2.4. Standardized management of email and instant messages ensures that information of business value is available when needed and is preserved according to established rules. It also provides access and security controls that support operational needs; supports efficient and effective search related to legal discovery and access to information and privacy requests; and reduces storage requirements.

2.5. A uniform approach to assigning email addresses, using email signature blocks, and defining the email properties applied to all Government of Jamaica email also helps maintain confidence and trust in government communications.

2.6. This standard is to be read in conjunction with the *Policy on Management of Information Technology* and the *Policy on Acceptable Network and Device Use*.

3. Definitions

3.1. Definitions to be used (Terms, Acronyms, etc.) in interpretation of this policy are provided in Section **11. Glossary Of Terms**.

4. Standard Statement

4.1. Objective

The objective of this Standard is to:

4.1.1. Ensure email and instant messages are managed efficiently, effectively, and in a timely manner to support business operations and decision making.

4.1.2. Provide organizations with the specifications to support the implementation of strong, consistent, and standardized email management practices.

4.2. Expected Results

The expected results of this policy are:

- Email and instant messages are effectively managed throughout their life cycle.
- Email services support program and service delivery.
- Email is identifiable as Government of Jamaica correspondence.

5. Standard Requirements

5.1. Permanent Secretaries / Heads Of Agencies

In the following areas, PSs / HOAs are responsible for ensuring that:

Information Management

5.1.1. appropriate corporate repositories for the storage of email and instant messages containing information of business value are designated;

5.1.2. dormant and deactivated email accounts are managed effectively, including the transfer of information of business value to designated corporate repositories and appropriate disposition;

5.1.3. appropriate liaison with the ICT Authority takes place to ensure compliance, performance management, and monitoring of the requirements of this standard, where email services are administered by the ICT Authority;

5.1.4. Appointing a Delegated Email Administrator where the ICT Authority administers email services on behalf of the department.

Specifications

5.1.5. email containing information of business value is transferred to designated corporate repositories in a timely manner by limiting individual email accounts to a maximum of 2 gigabytes (GB) of storage. Departments can provide additional increments of 1GB for specific cases, but are expected to limit exceptions to no more than 5 per cent of the total number of full-time employees in the organization;

5.1.6. access to all email containing information of business value by migrating email out of existing individual email archives (personal storage files, archives, etc.) into designated corporate repositories, and subsequently discontinuing the use of personal storage files and other email archives. Personal storage files may continue to be used for holding email as a result of access to information requests or for legal discovery purposes;

5.1.7. departmental software and systems are in place to create, manage, or store email and instant messages comply with the requirements of this standard or can be modified to meet the requirements.

Signature Blocks

5.1.8. email signature blocks are established in accordance with the requirements described in Appendix E.

5.1.9. all texts or disclaimers appended to employee and generic signature block email addresses. Email disclaimers must be limited to only those required for program or service delivery.

5.2. Email Administrator(s) is responsible for:

Note: *In departments where the ICT Authority administers email services, the ICT Authority is the Email Administrator.*

5.2.1. Where the ICT Authority administers email services on behalf of departments, ensuring that email addresses are established in accordance with the requirements described in Appendix B..

5.2.2. Where departments retain responsibility for email administration, ensuring that email addresses are established in accordance with the requirements described in Appendix C.

5.2.3. Ensuring that email properties are established in accordance with Appendix D.

5.2.4. Ensuring permanent disposition of email within the Deleted Items folder of each email account within 30 days.

5.3. The Delegated Email Administrator(s) is responsible for:

5.3.1. Requesting the creation and removal of email accounts by the ICT Authority.

5.3.2. Informing the ICT Authority of changes to the employment of email account holders prior to the effective date of the change. The responsibility for informing the ICT Authority of employee transfers from one department to another, when both departments' email services are administered by the ICT Authority, lies with the Delegated Email Administrator of the department to which the employee is transferring.

5.4. Managers are responsible for:

5.4.1. Ensuring that employees are aware of their responsibility to transfer email and instant messages of business value to designated corporate repositories as soon as possible.

5.4.2. Ensuring that employees have transferred all email and instant messages containing information of business value to designated corporate repositories prior to their departure or extended absence from the organization.

5.4.3. Ensuring that employees are aware of their responsibility to dispose of transitory email and instant messages as soon as they are no longer required.

5.4.4. Providing the organization's Delegated Email Administrators (or email administrator, in organizations where there is no Delegated Email Administrator) with information on any changes to employment of email account holders under their supervision prior to the effective date of the changes.

5.5. Employees are responsible for:

5.5.1. Ensuring that email and instant messages that contain information of business value are transferred to designated corporate repositories as soon as possible.

5.5.2. Ensuring that email and instant messages that contain information of business value are transferred to designated corporate repositories prior to their departure from the organization or any extended absence.

5.5.3. Ensuring that transitory information held in their email account or on their mobile devices is deleted as soon as possible according to approved disposition authorities.

5.5.4. Ensuring that information contained in the email signature block and the email properties is accurate and up-to-date.

6. Monitoring and Reporting Requirements

Permanent Secretaries / Heads Of Agencies

6.1.1. are responsible for monitoring adherence to this policy within their organizations, and for ensuring that appropriate remedial action is taken to address any deficiencies identified.

Government-wide

6.1.2. The ICT Council is responsible for:

a) oversight and monitoring of the compliance with this policy by permanent secretaries through an annual confirmation that policy requirements are being met, leveraging existing reporting mechanisms where applicable;
b) recommending that corrective action be taken when a MDA has not complied with the requirements of this policy; and
c) establishing a framework for the review of this policy and ensuring that a review is initiated within five years of the effective date of this policy.

7. Consequences

7.1. Consequences of non-compliance can include informal follow-ups and requests from ICT Council, external audits, and formal direction on corrective measures.

8. Management Roles and Responsibilities

8.1. The ICT Authority is responsible for:

8.1.1. Developing standards, guidelines and tools for email management; and

8.1.2. the management and operation of the common and shared IT services in consultation with MSET and the ICT Council, which includes those that meet the requirements of this standard related to email and end-user devices.

8.2. The ICT Council is responsible for:

8.3. Providing interpretive advice and guidance on this standard;

8.4. Providing support to Information Management Senior Officials and/or other committees and working groups, as necessary, to address government-wide challenges and opportunities in implementing this standard and supporting instrumentsProviding support to Information Management Senior Officials and/or other committees and working groups, as necessary, to address government-wide challenges and opportunities in implementing this standard and supporting instruments.

9. Enquiries

9.1. The ICT Council is responsible for the policy instruments supporting this policy framework; please direct any enquiries to:

Chief Information Officer

Office of the CIO

(876) 929-8990 - 9
(876) 960-1623
cio@mset.gov.jm

10. References

10.1. Relevant Legislation

- Data Protection Act (under development)

11. Glossary Of Terms

company name

An email property that associates the name of the email sender's home department to the email address. This property is found under Email Properties.

deactivated email account

An email account that is no longer required. The email account can no longer send or receive emails. The reason may be, for example, that the employee has left the organization or that the program relating to the generic account has ended.

Delegated Email Administrator

An individual who has been delegated authority for administrative access to the ICT Authority's Email Solution Service.

display name

An email property that enables email users to see the name of an individual, program or service for any given email address. The display name is the name that email recipients see in their email inbox and on printed emails, and that is used in address directories. This property is found under Email Properties.

dormant email account

An email account that is temporarily suspended. For example, this may be the email account of an individual on extended leave.

electronic mail

See **Email**.

email

A message sent and received in electronic form via computer networks or a computer system.

email account

An email mailbox and the associated rights to use that mailbox.

email address

The character string used to allow computer systems to route an email message to the intended email account, usually consisting of a username, the @ symbol and a domain name. (Library and Archives Jamaica, *Email Management Guidelines*)

email address prefix

Portion of the email address before the @ symbol.

email address suffix

Portion of the email address after the @ symbol.

Email Administrator

An individual or entity who is responsible for the configuration and management of an email service.

email client

An application or program that allows the user to compose, read and send email. An email client may be on the Web, a computer desktop, a mobile device or other technology.

email disclaimer

A statement that is appended to an email.

email domain name

A unique address that comes after the @ symbol in an email address. A domain name may or may not include a sub-domain name.

email property

One configurable piece of information used by an email service and an email client to assist in identifying the sender of email. It is made available through the address book and the active directory. An email property is a subset of Email Properties.

email service

A service offered by an organization that enables users to create, transmit, receive, respond to, and store email. An email service is accessed by an email client.

generic email address

An email address that is not linked to an individual; instead, it is linked to a program or service or used for resource management.

instant message

A message, other than email, sent and received electronically in real time via mobile devices or computer networks, which enables users to create, transmit, receive and respond to messages electronically.

mailbox

The area in a computer system where the incoming and outgoing email messages, calendar entries, task items, contacts and journal entries for an email account are stored.

personal storage file

A file that contains messaging objects. This includes .pst files from Microsoft Exchange, .nsf files from IBM Lotus Notes and Domino, and .db files from Novell GroupWise.

This Page Intentionally Left Blank

12. Appendices

Appendix A: Naming Conventions for Email Addresses Administered by the ICT Authority

the ICT Authority is responsible for ensuring that email sent from email services administered by Shared Service Jamaica complies with the requirements described in this appendix.

Domain Name

- *gov.jm* is to be applied in the email address suffix as the primary email domain name to clearly identify Government of Jamaica email communications.

Enterprise Email Addresses

- For the purposes of official external correspondence, departments may request, subject to ICT Authority approval, the creation of a GC enterprise email address that is not linked to a department or individual employee.
- Enterprise email addresses may be established for Government of Jamaica priorities and/or cross-mandate programs and services.
- Conflicts may arise in naming enterprise email addresses. In these situations, it is up to the Email Administrator to resolve such conflicts.
- Departments may choose one of the options below for enterprise email addresses:

  The email address may include a descriptor.

  Model:
  Descriptor@gov.jm

  Example:
  Blueprint2020@gov.jm

  Model:
  Descriptor@gov.jm

Example:
Blueprint2020@gov.jm

Requests for specific enterprise email addresses with a rationale for creating the address must be submitted to the ICT Authority..

Email address for individual email accounts

PreferredName.LastName is the naming convention to be applied. The preferred name can be a first or middle name.

Model: PreferredName.LastName@gov.jm

Example: john.jamaican@gov.jm

Duplicate email accounts and tiebreaker rules

Where a conflict exists for the use of a particular name, a numerical tiebreaker is to be applied immediately after the last name. Numerical tiebreakers start with the number 2. Subsequent tiebreaker numbers are to be applied sequentially.

Model: PreferredName.LastName#@gov.jm

Example: jane.jamaican2@gov.jm

Government of Jamaica email addresses become available for reuse as needed after a period of two years.

Email addresses for generic programs and services or other uses

Generic email addresses

For the purpose of official correspondence, a department may establish a generic email address that is not linked to an individual employee:

- For the use of a departmental program or service; and
- For the purposes of resource management, including boardrooms, vehicles and equipment.

Conflicts may arise in naming email addresses. In these situations, it is up to the Email Administrator to resolve such conflicts.

Generic email addresses for programs or services

Generic email addresses for programs or services must include the departmental abbreviation.

The email address must also include a descriptor for the program or service.

The departmental abbreviation and the program or service descriptor are to be separated by a period.

Model: Dept.Descriptor@gov.jm

Generic email addresses for resources

Generic email addresses for the purpose of resource management must include the departmental abbreviation.

The email address must include the resource type as defined by the ICT Authority. A period is to be used to separate the resource type and the departmental abbreviation.

Model: Dept.ResourceType-DescriptorMin@gov.jm

Appendix B: Naming Conventions for Email Addresses Administered by Departments

Departmental email administrators are responsible for ensuring that email sent from email services administered by their department complies with the email address requirements described in this appendix.

The following requirements apply:

Domain Name

- *gov.jm* is to be applied in the email address suffix as the primary email domain name to clearly identify Government of Jamaica email communications.

Email addresses for individuals

PreferredName.LastName is the naming convention to be applied. The preferred name can be a first or middle name.

Model: PreferredName.LastName@DepartmentDomainName.gov.jm

Implement duplicate email accounts and tiebreaker rules. The preferred tie breaker rules are outlined in Appendix A.

Email addresses for generic programs and services or other uses

A department may establish a generic email address that is not linked to an individual employee:

- For the use of a departmental program or service; and
- For the purposes of resource management, including boardrooms, vehicles and equipment.

The preferred naming convention for establishing a generic email address prefix is outlined in Appendix A.

Conflicts may arise in naming email addresses. In these situations, it is up to the email administrator to resolve such conflicts. The preferred tie breaker rules are outlined in Appendix A.

Appendix C: Email Properties

The requirements described in this appendix are applied by the email administrator (the ICT Authority or departmental email administrators in departments that administer their own email service).

Email properties provide information used by email services and email clients to assist in identifying the sender of email.

The "display name" for individuals and generic email addresses is an email property that recipients see when an email is received and on printed email messages. The "company name" is the email property that associates the name of the sender's home organization to the email address.

The display name property may also be used in directories. The email administrator may establish additional display names that resolve to a single email address for use in directories.

Display name property

Display name for email addresses for individuals

The display name **must** contain the elements below:

- Full name and numerical tiebreaker, if the email address has one;
- Approved abbreviation of the MDA, and

The full name and department abbreviation must be displayed as follows:

- LastName, PreferredName (Dept/Min.); or
- LastName#, PreferredName (Dept/Min.), when the email address has a numerical tiebreaker.

The Display name **may** also contain the rank of the individual where the rank is a requirement for the continuation of the performance of the duties of the employee's position.

No other elements may appear in the display name.

Display name for generic email addresses for programs and services

The display name for email accounts **must** contain the elements below:

- The name of program or service; and
- Approved abbreviation of departments

The display name for a program or service **must** be displayed as follows:

- Name of Program or Service

No other elements may appear in the display name.

Display name for generic email addresses for resource management

The display name for generic email accounts for resource management **must** contain the elements below:

- Approved abbreviation of MDAs;
- The resource type, as defined by the email administrator, and
- A unique identifier for the resource

The display name for a resource **must** be displayed as follows:

- **Dept ResourceType ResourceIdentifier**

Company name property

The company nameproperty **must** contain the elements described below:

- Applied title of the department of the individual, program or service.

Appendix D: Email Signature Blocks

Information Management Senior Officials are responsible for ensuring that email signature blocks comply with the requirements described herein.

Email signatures must be applied to all emails sent, including replies.

Components and layout of signature blocks for individuals

Signature blocks for individuals must contain the elements described below:

- **Line one**: The sender's name, which may include a rank or a designation when the rank or designation is a requirement for the continuation of the performance of the duties of the employee's position.
- **Line two**: No content (empty line).
- **Line three**: The sender's title and departmental branch.
- **Line four**: The department's applied title.
- **Line five**: Email address and telephone numbers.
    - The telephone number must appear with the area code in the following format:
        - (876) 999-1234, including an extension number where applicable.
        - Preceded by "Tel:".
        - Cellular numbers provided on government-approved devices such as cellular phones, smart phones and other devices can be included:
            - As the primary telephone number and identified by the abbreviation "Tel:"; or
            - As a secondary telephone number and identified by the abbreviation "Cel:".
- **Line six**: No content (empty line).
- **Line seven**: The department's applied title and the words "Government of Jamaica".
- **Line eight**: No content (empty line).
- **Line nine**: Approved disclaimer text, if applicable.

The same requirements are to be applied to email clients on mobile devices, technology permitting.

Components and layout of signature blocks for generic email accounts

The signature block must contain the elements described below:

- **Line one**: The program or service name for an email from a generic email account.
- **Line two**: The department's applied title.
- **Line three**: Email address and telephone.
    e. The telephone number must appear with the area code in the following format:
        i. 876-999-1234, including an extension number where applicable.
        ii. Preceded by "Tel:".
        iii. Cellular numbers provided on government-approved devices such as cellular phones, smart phones and other devices can be included:
            1. As the primary telephone number and identified by the abbreviation "Tel:"; or
            2. As a secondary telephone number and identified by the abbreviation "Cel:".
- **Line four**: No content (empty line).
- **Lines five and six**: The Government of Jamaica signature and the MDA identifier, technology permitting.

- **Line seven**: No content (empty line).
- **Line eight**: Approved disclaimer text, if applicable.

The same requirements are to be applied to email clients on mobile devices, technology permitting.

Presentation of the signature block

- Email disclaimers are to be applied only when required to address program or service needs.
- Additional elements beyond the requirements must not be added to signature blocks. This includes the space immediately above or below an email signature block.
- Departments must ensure that email signature blocks avoid the appearance or public perception of providing an endorsement or marketing subsidy or an unfair competitive advantage, as per the Policies of the Government of Jamaica.

Examples

Email addresses and signatures for individuals – email services administered by the ICT Authority

No tiebreaker rules applied to email address

Line 1	John jamaican
Line 2	*(No content – empty line)*
Line 3	Analyst, Office of the Chief Information Officer
Line 4	ICT Council / Government of Jamaica
Line 5	john.jamaican@gov.jm / Tel: 876-955-5555 / TTY: 876-955-5556
Line 6	*(No content – empty line)*
Line 7	*Disclaimer text, if applicable*

Numerical tiebreaker rule applied to email address

Line 1	John jamaican
Line 2	*(No content – empty line)*
Line 3	Analyst, Chief Information Officer Branch
Line 4	ICT Council / Government of Jamaica
Line 5	john.jamaican2@gov.jm / Tel: 876-955-5555 / TTY: 876-955-5556
Line 6	*(No content – empty line)*

Generic program or service – email services administered by the ICT Authority

Line 1	HR Services / Human Resources Department
Line 2	ICT Council / Government of Jamaica
Line 3	tbs.hr-rh.sct@gov.jm / Tel: 1-800-999-1234 / TTY: 876-955-5556
Line 4	*(No content – empty line)*
Line 5	*Disclaimer text is applied, if applicable*

Email account for individual – email service administered by department

Line 1	John jamaican
Line 2	*(No content – empty line)*
Line 3	Analyst, Office of the Chief Information Officer
Line 4	Department / Government of Jamaica
Line 5	john.jamaican@DeptDomainName.gov.jm / Tel: 876-955-5555 / TTY: 876-955-5556
Line 6	*(No content – empty line)*
Line 7	*Disclaimer text is applied, if applicable*

Generic program or service – email service administered by department

Line 1	HR Services / Chief Human Resources Office Branch
Line 2	Department / Government of Jamaica
Line 3	dept.hr-rh.min@DeptDomainName.gov.jm / Tel: 1-800-999-1234 / TTY: 876-955-5556
Line 4	*(No content – empty line)*
Line 12	*Disclaimer text is applied, if applicable*

This Page Intentionally Left Blank

Standard for Electronic Documents and Records Management Solutions (EDRMS)

1. Application

1.1. This standard applies to all MDAs of the Government of Jamaica.

1.2. The Permanent Secretaries through the various IT heads of these MDAs are solely responsible for monitoring and ensuring compliance with this standard within their organizations, as well as for responding to cases of non-compliance in accordance with any instrument issued by the office of the Chief Information Officer.

2. Context

2.1. This standard supports the *Policy on Information Management* and *Policy on Management of Information Technology* by outlining information management (IM) and information technology (IT) requirements for ministries in their Electronic Document and Records Management (EDRM) solutions.

2.2. Information resources of business value are strategic assets used across government to support effective decision making and facilitate ongoing operations and the delivery of programs and services. Ministries are required to establish the mechanisms and tools to support the ministries' recordkeeping requirements throughout the information life cycle.

2.3. EDRM solutions are automated systems used to manage, protect and preserve information resources from creation to disposition. These solutions maintain appropriate contextual information (metadata) and enable organizations to access, use and dispose of records (i.e., their retention, destruction or transfer) in a managed, systematic and auditable way in order to ensure accountability, transparency and meet departmental business objectives.

2.4. EDRM solutions may be a part of a suite of products that, along with effective policies and practices, enable a ministry-wide approach to information management that improves the

quality and reliability of information for decision-making, improves services to managers and employees, and reduces inefficiencies, duplication and costs.

2.5. Through the implementation of government-wide IM business processes and practices and the use of government-wide procurement options in support of EDRM solutions, the government will see a reduction in the overall cost of service delivery.

2.6. Investment decisions to acquire EDRM solutions resulting from government-wide procurement activities may be combined with other departmental solutions to provide a more comprehensive product suite.

2.7. EDRM solutions enable GC employees to find, share and collaboratively develop information resources of business value, therefore increasing their productivity, and the efficiency and effectiveness of their departments.

3. Definitions

3.1. Definitions to be used in the interpretation of this standard are contained in Section **9. Glossary of Terms**.

4. Standard Statement

4.1. Objectives

4.1.1. To support efficient and effective management of information through the use of EDRM solutions to increase timely access to relevant, reliable, and comprehensive information to support decision-making in program and service delivery.

4.1.2. To maximize the benefit of GoJ investments related to EDRM solutions by reducing the overall cost associated with implementation and ongoing operations through standardization and economies of scale.

4.2. Expected Results

4.2.1. Increased government-wide access to information within and across ministries to enable increased employee productivity and the efficiency and effectiveness of program and service delivery to Jamaicans;

4.2.2. Increased use of common or shared information and technology solutions, assets, and services in support of EDRM solutions, in order to avoid duplication, reduce costs and leverage partnership opportunities.

5. Requirements

5.1. The Head of Agency is responsible for:

5.1.1. Ensuring that investment decisions which pertain to the acquisition of EDRM solutions maximize the use of products and services made available as a result of government-wide procurement processes, as described in Appendix A.

5.1.2. Ensuring common, consistent, and cost effective ministerial implementation of EDRM solutions to meet recordkeeping requirements.

5.1.3. Ensuring that EDRM solutions meet a defined set of standard requirements, as described in Appendix C.

5.2. Monitoring and reporting requirements are as follows:

Permanent Secretaries / Heads of Agencies

5.2.1. These executives are responsible for monitoring adherence to this policy within their organizations, and for ensuring that appropriate remedial action is taken to address any deficiencies identified.

Government-wide

5.2.2. The ICT Council is responsible for:

a) oversight and monitoring of the compliance with this policy by permanent secretaries through an annual confirmation that policy requirements are being met, leveraging existing reporting mechanisms where applicable;
b) recommending that corrective action be taken when a MDA has not complied with the requirements of this policy; and
c) establishing a framework for the review of this policy and ensuring that a review is initiated within five years of the effective date of this policy.

6. Consequences

6.1. Consequences of non-compliance are in accordance with existing practices within the GoJ and can include informal follow-ups and requests from ICT Council, external audits, and formal direction on corrective measures.

7. Roles and Responsibilities of Government Organizations

7.1. The Office of the Chief Information Officer

7.1.1. The Office of the CIO provides guidance on this Standard;

7.1.1.1. gives interpretive advice on this Standard;

7.1.1.2. develops and promotes, in consultation with other central government ministries, a program and framework for the management of information; enterprise information architecture, including principles, methods, processes and standards, to enable consistent information architecture across domains such as finance, human resources, etc., as well as standards, procedures, directives, guidelines, tools, and best practices that achieve the goals and expected results of this policy;

7.1.1.3. promotes functional communities for the management of information as required to develop and sustain information management functional specialist capacity and practices; and

7.1.1.4. develops competency and other professional standards for information management functional specialists as required.

7.2. The Ministry of Education, Youth & Information

The Ministry of Education, Youth & Information is the portfolio Ministry responsible for collecting and archiving information, and, in the case of this Standard:

7.2.1. acquires, preserves, makes known and facilitates access to the documentary heritage of Jamaica;

7.2.2. preserves the published heritage of the nation and of the Government of Jamaica;

7.2.3. provides direction and assistance on recordkeeping for the Government of Jamaica;

7.2.4. identifies, selects, acquires and preserves government records in all media considered to be of enduring value to Jamaica as documentary heritage

7.2.5. issues records disposition authorities, to enable ministries to carry out their records retention and disposition plans;

7.2.6. manages and protects the essential records and less frequently referenced material of Government Ministries; and

7.2.7. Assists Government Ministries in ensuring that all of their published information is easily accessible to decision makers and is available to the public.

8. Enquiries

8.1. The ICT Council is responsible for the policy instruments supporting this policy framework; please direct any enquiries to:

Chief Information Officer

Office of the CIO

(876) 929-8990 - 9
(876) 960-1623
cio@mset.gov.jm

9. Glossary of Terms

EDRM solutions

Are automated systems used to manage, protect and preserve information resources creation to disposition. These solutions maintain appropriate contextual information (metadata) and enable organizations to access, use and dispose of records (i.e., their retention, destruction or transfer) in a managed, systematic and auditable way in order to ensure accountability, transparency and meet ministerial business objectives.

Information life cycle

The life cycle of information management encompasses the following: planning; the collection, creation, receipt, and capture of information; its organization, use and dissemination; its maintenance, protection and preservation; its disposition; and its evaluation.

Information resources

Any documentary material produced in published and unpublished form regardless of communications source, information format, production mode or recording medium. Information resources include textual records (memos, reports, invoices, contracts, etc.), electronic records (emails, databases, internet, intranet, data etc.), new communication media (instant messages, wikis, blogs, podcasts, etc.), publications (reports, books, magazines), films, sound recordings, photographs, documentary art, graphics, maps, and artefacts.

Information resources of business value

Are published and unpublished materials, regardless of medium or form, that are created or acquired because they enable and document decision-making in support of programs, services

and ongoing operations, and support ministerial reporting, performance and accountability requirements.

Information technology

Includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation and implementation of information systems and applications to meet business requirements.

Investment

Is the use of resources with the expectation of a future return, such as an increase in output, income or assets, or the acquisition of knowledge, or capacity.

Management of information technology

Includes planning, building (or procuring), operating and measuring performance.

Metadata

The definition and description of the structure and meaning of information resources, and the context and systems in which they exist.

Record

For the purpose of this standard, records are information created, received, and maintained by an organization or person for business purposes, legal obligations, or both, regardless of medium or form.

Recordkeeping

A framework of accountability and stewardship in which information resources are created or acquired, captured, and managed as a vital business asset and knowledge resource to support effective decision-making and achieve results for Jamaicans.

Repository(ies)

A repository is a preservation environment for information resources of business value. It includes specified physical or electronic storage space and the associated infrastructure required for its maintenance. Business rules for the management of the information resources captured in a repository(ies) need to be established, and there must be sufficient control for the resources to be authentic, reliable, accessible and usable on a continuing basis.

10. Appendices

Appendix A: Investment

When investing in an EDRM solution, ministries are required to use products, licenses, or services resulting from government-wide procurement processes.

Investment in EDRM solutions is subject to the requirements of this standard whether the purpose of the investment is the implementation of a new EDRM solution, the replacement of an existing EDRM solution, or a significant upgrade to an existing solution.

- Significant upgrade refers to increases in the number of users greater than 100% of the initial planned implementation of the existing solution and/or functional improvements which exceed the original functionality of the existing solution, and **not** activities related to regular operational maintenance (e.g. bug fixes) or incremental system upgrades (e.g. version 1.1 to version 1.2).

The ministry IM Senior Official is responsible for submitting a justification for any proposed alternative to the products or services made available as a result of government-wide procurement processes. The justification is to be provided to the Government of Jamaica's Chief Information Officer prior to any investment.

The justification should include: the Ministerial IM Strategy and implementation plan, and be accompanied by a strong rationale (including cost effectiveness) to support the proposed alternate solution.

Appendix B: Requirements for EDRM Solutions

The International Council on Archives *Principles and Functional Requirements for Records in Electronic Office Environments - Module 2* requirements are the minimum requirement set to support the Government of Jamaica Electronic Document and Records Management implementation.

International Council on Archives, *Principles and Functional Requirements for Records in Electronic Office Environments - Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems*, 2008, published at www.ica.org.

Standard for Operational Security

PART I

Introduction to the Standard

Purpose
This standard defines baseline security requirements that Government Ministries, Departments, and Agencies (MDAs) must fulfill to ensure the security of information and information technology (IT) assets under their control.

Scope and Application
IT security is defined as the "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information." For the purposes of this standard, the term 'IT security' will also include the safeguards applied to the assets used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy information electronically.

Risk Management Philosophy
This standard establishes requirements for IT security, though the implementation of these requirements is to be managed by MDAs. Technical documentation, issued pursuant to this standard, will provide further implementation guidance.

Principles

Service delivery requires IT security.
IT security is an integral part of continuous program and service delivery. To avoid the loss of service and trust that IT security breaches can cause, MDAs need to view IT security as a business imperative; a "service enabler."
Although program and service delivery managers may delegate responsibility for IT security to technical experts, they remain accountable to their MDA Head and are responsible for ensuring the security of the programs and services under their authority.

IT security practices need to reflect the changing environment.
Information technology continues to rapidly advance in support of greater interconnectedness and improved service delivery. At the same time, the number and potential severity of threats, vulnerabilities and incidents similarly increase. Government ministries, department, and public sector agencies need to be aware of this evolving environment, and understand how to manage their IT security programs in order to respond.

The Government of Jamaica is a single entity.
The increased availability of common and shared services can help MDAs to meet their security requirements and better serve the Jamaican people. While this offers the potential for improved efficiency, MDAs have to recognize that the security decisions they make can impact other organizations.

Working together to support IT security.
Far more than the sum of the tools used to protect information and systems, an effective IT security program combines people, processes and technologies. Each MDA's senior managers, program and service delivery managers, security personnel, IT operational personnel, human resources personnel and other stakeholders work together in a concerted manner to achieve the same high level of IT security across the central government.

Decision-making requires continuous risk management.
In order to make sound decisions based upon risk management, MDAs need to continually be aware of the assets they hold, and their associated sensitivity and criticality. Decisions should be made based upon risk management that recognizes the potential impacts to the MDA and to government as a whole.

Structure of This Standard

This standard has three major parts, plus appendices. Part I provides general information on IT security. Part II provides direction on the organization and management of IT security within Government ministries, department, and public sector agencies. Part III provides direction on technical and operational safeguards.

Appendix A of this Standard defines the roles and responsibilities of MDAs that play a lead role in information and IT security within the Government.

PART II

IT Security Organization and Management in MDAs

Introduction

This part of the standard provides direction and guidance on how to organize and manage a departmental IT security program. It covers roles and responsibilities, policy, resources and management controls.

Roles and Responsibilities

Although MDAs differ in how they assign the following roles and responsibilities (e.g. they may use different titles than those indicated), each MDA must designate individuals to perform the *functions* noted in this section. The Minister may, in cases where there are numerous sub-agencies and department, appoint deputies for each role listed below to assist in offsetting the workload and improve efficiency.

IT Security Coordinator

MDAs must appoint an IT Security Coordinator with at least a functional reporting relationship to the Cluster Chief Information Officer and the Senior ICT Officer in the MDA.

At a minimum, the IT Security Coordinator must

1. Establish and manage a MDA IT security program as part of a coordinated MDA security program,
2. Review and recommend approval of MDA IT security policies and standards, and all policies that have IT security implications,
3. Ensure review of the IT security related portions of Request for Proposals and other contracting documentation, including Security Requirements Checklists,
4. Recommend approval of all contracts for external providers of IT security services,
5. Work closely with program and service delivery managers to
    - ensure their IT security needs are met,
    - Provide advice on safeguards,
    - advise them of potential impacts of new and existing threats, and
    - advise them on the residual risk of a program or service,
6. Monitor ministries' compliance with this standard and associated documentation,
7. Promote IT security in the MDA,
8. Establish an effective process to manage IT security incidents, and monitor compliance with it, and
9. Serve as the department's principal IT security contact.

The IT Security Coordinator position must be screened with very high scrutiny. In hiring for this

position, ministries should give preference to individuals with appropriate professional certification.

Senior Management

One of the roles of senior management is to foster a "culture of security" across the MDA.

When defining the MDA's priorities, strategic directions, program objectives, budget and personnel allocations, senior management must address IT security requirements. Senior management must also ensure adequate funding for security in IT projects

Senior management must approve MDA IT security policies, standards and directives.

MDA Security Officer

This standard requires Ministries to appoint a MDA Security Officer to establish and direct a departmental security program, and provides a list of their responsibilities.

The Departmental Security Officer and the IT Security Coordinator must ensure that physical, personnel and IT security stakeholders coordinate their efforts to protect information and IT assets and ensure an integrated, balanced approach.

Chief Information Officer

The MDA's Chief Information Officer is responsible for ensuring the effective and efficient management of the department's information and IT assets. Given the potential impact of service delivery failures due to security breaches, the Chief Information Officer and the IT Security Coordinator must work together to ensure that appropriate security measures are applied to all Ministries' Information Management and IT assets, activities and processes.

Business Continuity Planning Coordinator

The Chief Information Officer, MDA Security Officer, IT Security Coordinator and the Business Continuity Planning Coordinator must work together to ensure a comprehensive approach to continuous service delivery.

Program and Service Delivery Managers

On behalf of the heads of ministries, program and service delivery managers are responsible for ensuring an appropriate level of security for their programs and services. In designing programs and services, managers will work with MDA security specialists to risk manage their programs or services. Relying on the advice and support of the IT Security Coordinator, managers must determine the IT security requirements of their programs and services, have them accredited, and accept the associated residual risk.

IT Operational Personnel

IT operational personnel includes network or system administrators or managers, help desk personnel, account managers, system security, maintenance and all other IT support personnel. Under the general

direction of the IT Security Coordinator and in accordance with MDA priorities, policies and procedures, IT operational personnel must

- follow security procedures and recommend improvements to them,
- respond to security incidents,
- test and install security patches,
- maintain or upgrade security hardware and software,
- monitor systems and logs,
- back up and recover information, and
- manage access privileges and rights.

Other Personnel

All personnel must abide by the Government's and the MDA's IT security policy, procedures and other related documentation. They must report real and suspected security incidents to designated security officials, normally through their immediate supervisor. For the purpose of this standard, personnel include employees, staff, contractors, students, visitors, and Jamaican Security Forces.

IT Project Managers

With guidance from the IT Security Coordinator and IT operational personnel, IT project managers must ensure that project security requirements are met through the development and implementation of technical security specifications.

Departmental IT Security Policy

Every MDA must have an IT security policy in accordance with this standard and other related policies, standards and technical documentation. This may be a separate document or it can be policy statements within the MDA security policy.

As a minimum, an MDA IT security policy must

- define the roles and responsibilities of program and service delivery managers, the Chief Information Officer, MDA's legal, privacy specialists and security specialists, and other personnel with regard to IT security
- make the necessary connections with other MDA policies, standards, and legal and regulatory requirements that relate to IT security
- state the requirement for making IT security an integral part of program and service delivery
- state a requirement for seeking funding in support of IT security requirements,
- state requirements for the review and revision of the MDA's IT security policy and supporting documentation.

I.T Security Resources for Projects

In planning new programs, services or major upgrades to existing programs or services, the managers responsible must, at the earliest stage of the funding and approval process, determine the IT security requirements for these programs, services or upgrades and include resource requirements in funding requests.

Management Controls

This section describes the management controls that apply to all Ministries' programs and services. Part III of this standard defines the technical and operational safeguards that support these controls.

Security in the System Development Life Cycle

Given the difficulty of implementing cost-effective IT safeguards after a system has been deployed and because technologies and threats continuously change, ministries must address security and adjust security requirements throughout all the following stages of the system development life cycle, including at the earliest stages of planning and review:

1. Initiation
   An initial Threat and Risk Assessment will provide input for IT security requirements.

2. Design and Development
   An appropriate balance of technical, managerial, operational, physical and personnel security safeguards will help to meet the requirements determined by the Threat and Risk Assessment.

3. Implementation
   Design documentation, acceptance tests, and certification and accreditation are to be performed.

4. Operation
   System security is monitored and maintained while Threat and Risk Assessments aid in the evaluation of modifications that could affect security.

5. Disposal
   In accordance with archival and security standards and guidelines, archive or dispose of sensitive IT assets and information resident on the system.

Given that systems underlie most programs and services, the system development life cycle approach to IT security also applies to the management of programs and services.

Security Risk Management

Departments must continuously manage the security risks to information and IT assets throughout the life of their programs and services.

Security risk management activities include Threat and Risk Assessments, audits, Business Impact Analysis, Privacy Impact Assessments, self-assessments, monitoring, security investigations, and Vulnerability Assessments. Given that some of these activities will generate the same or similar risk management information, the program or service delivery manager should avoid duplication by ensuring that these activities are coordinated and that the information garnered from them is shared (in accordance with laws and policies dealing with the collection, use, disclosure and retention of information).

Graduation of Controls and Safeguards

- The graduated application of management controls and technical and operational safeguards should be based upon at least the following:
- The sensitivity and criticality of related program or service assets,
- Threats to asset confidentiality, integrity, availability or value,
- Known vulnerabilities for the program or service,
- Incident data or history,
- Exposure of assets to threats (e.g. exposure to the Internet).

These activities contribute to the risk management of programs, systems and services.

Threat and Risk Assessment

A Threat and Risk Assessment aids in the determination of security requirements. Departments must apply security measures above baseline levels when justified by a Threat and Risk Assessment.

The steps of a Threat and Risk Assessment are to

- identify and categorize information and related assets according to their sensitivity (noting this information in a "Statement of Sensitivity"),
- assess the threats and system vulnerabilities that could affect the delivery of a program or service,
- determine the level of risk, based on current safeguards and system vulnerabilities, and
- recommend safeguards that will mitigate risk to an acceptable level.

Ministries must conduct a Threat and Risk Assessment for every program, system or service. Threat and Risk Assessments can be short and simple or far more detailed and rigorous, depending on the sensitivity, criticality and complexity of the program, system or service being assessed.
For programs, systems or services in which the operating environment and security concerns are the same or similar, ministries are encouraged to develop "generic" Threat and Risk Assessments that can be reused.

Certification and Accreditation

The purpose of certification is to verify that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended. The purpose of

accreditation is to signify that management has authorized the system or service to operate and has accepted the residual risk of operating the system or service, based on the certification evidence.

Ministries must have their systems or services certified and accredited before approving them for operation. The graduated performance of certification depends upon the quantity and quality of certification evidence required by the accreditation authority. Such evidence can include the results of any applicable Threat and Risk Assessment, a Business Impact Assessment, a Privacy Impact Assessment, a Vulnerability Assessment, security tests and product evaluation, self-assessments, audits and security reviews and related legal or policy assessments that demonstrate conformance to relevant legislation or policy.

Ministries must periodically review the accreditation of systems or services if the systems or services have changed significantly or if warranted due to changes in the risk environment.

For common systems or services, the Government of Jamaica's Chief Information Officer is the accreditation authority. For systems or services that are specific to a MDA, the program or service delivery manager is responsible for accreditation. For systems or services shared by two or more organizations, the manager of the program or service is the accreditation authority.

Incident Management

Incident management consists of the management of incidents from their discovery to the implementation of appropriate responses. Incident discovery is often implemented through systems that detect incident occurrence. Once detected, ministries need to be able to properly identify and respond to the incident, both within their ministries and as part of a coordinated response across government.

Vulnerability Management

Ministries must continuously manage vulnerabilities for their programs, systems and services. This management task includes the discovery of vulnerabilities, and the implementation of corresponding solutions. As part of discovery, ministries must actively review sources of vulnerability information to determine the potential effect on their programs, systems and services.

As part of solution management, ministries must determine the risk posed by vulnerabilities. Based upon this risk, ministries should test the impact of the proposed solution to the vulnerability, and subsequently implement and deploy the solution (e.g. software patch). Ministries that discover a system vulnerability for which there is no patch should use another method to mitigate the risk (e.g. configuration change).

Vulnerability Assessments

A Vulnerability Assessment supports the discovery of vulnerabilities in existing systems. Ministries must conduct a Vulnerability Assessment regularly on highly sensitive or highly exposed systems, and on a discretionary basis on other systems.

Ministries must document Vulnerability Assessments, subsequent decisions and remedial actions, e.g. software patches.

Patch Management

The failure to promptly apply security-related patches can lead to serious IT security incidents. Ministries must establish a systematic, documented patch management process to ensure they apply security-related patches in a timely manner. The IT Security Coordinator must ensure that this process is effective and that the MDA follows it.

Segregation of Responsibilities

Assigning all responsibilities related to an IT system or business function to a single individual can make a system vulnerable to undetected abuse or a single point of failure. To ensure that no single person has complete control of an entire IT system or a major operational function, ministries must segregate IT responsibilities as much as possible. Individuals who are authorized to conduct sensitive operations must not be allowed to audit these operations.

Contracting

Ministries need to address IT security requirements in the contracting process. Before issuing a contract, ministries must ascertain if IT security is relevant to the goods or services to be provided by the contractor, and if so, account for the security requirements at every stage of contracting.
Ministries must identify individuals within the department to oversee the work of external IT security service providers.

Continuity Planning

Information management (IM) continuity planning and information technology (IT) continuity planning are integral elements of business continuity planning. One of the objectives of IM continuity planning is to ensure minimal or no interruption in the availability of information assets. One of the objectives of IT continuity planning is to ensure minimal or no interruption in the availability of critical IT services and assets. As part of their business continuity planning, departments must produce and routinely test and revise an IM continuity plan and an IT continuity plan. The Business Continuity Planning Coordinator must collaborate with the IT Security Coordinator throughout business continuity planning.

Sanctions

Departments are required to apply sanctions to IT security incidents when in the opinion of the head of the MDA, there has been misconduct or negligence.

Sharing and Exchange of Information and I.T Assets

Ministries that share information, I.T infrastructure or other I.T assets must establish a written security arrangement that defines the terms and conditions of any authorized sharing, and recognize any legal impediments to the sharing. Ministries that share information or other assets or use common infrastructure must conform to the security standards defined for that system or infrastructure.

Ministries that hold or use information from outside the Government of Jamaica must respect existing agreements or arrangements with the parties that have provided the information.

MDA I.T Security Assessment and Audit

Ministries need to actively monitor their management practices and controls. As part of this responsibility, departments assess and audit IT security and remedy deficiencies where necessary.

Self-Assessment

Ministries must conduct an annual assessment of their IT security program and practices to monitor compliance with government and MDA security policies and standards.

The IT Security Self-Assessment will identify deficiencies and help Ministries recognize and implement remedial action. Based on the results of this self-assessment, Ministries must develop or update their IT security action plan and determine the resources required to implement it.

To help the CIO assess the state of security across government, Ministries must submit their IT Security Self-Assessment whenever the Government's Chief Information Officer requests it.

Internal Audit

Planning for IT security audits must be incorporated into the overall MDA internal audit planning process, MDA and Government of Jamaica requirements and the overall MDA risk management strategy and practices. In general, the internal audit planning process assigns priority to the areas of higher materiality and risk, fundamental MDA financial, administrative or control systems and external performance reporting processes.

The IT Security Coordinator and the Chief Information Officer must be consulted during each phase of any audit of the IT security program, and in all audits of MDA programs or services that have an IT security component. The IT Security Coordinator must prepare a written response to the IT security audit and develop an action plan for senior management approval.

I.T Security Awareness

Ministries must inform and regularly remind personnel of IT security responsibilities, concerns and issues. These personnel include all those with access to the governmental information and IT assets. Ministries must provide IT security awareness in their employee orientation training. Ministries should incorporate IT security awareness into their broader MDA security awareness program.

Ministries must ensure that all personnel know of the security risks associated with computers at workstations and other equipment (e.g. Personal Digital Assistants - PDAs), given that the security of the information accessed depends primarily on the person using the equipment.

To increase employee awareness, Ministries are encouraged to post notices about IT security in all areas where personnel work, and check workstations routinely to ensure personnel are respecting IT security practices

I.T Security Training
Ministries must provide ongoing IT security training to all individuals with significant IT security responsibilities.

Part III

Technical and operational safeguards

Part III provides direction and guidance on some of the technical and operational safeguards that are available. Ministries select a combination of these and potentially other safeguards that together reduce the residual risk to an acceptable level. Additional safeguards are described in other security standards and technical documentation.

Graduated Safeguards
Ministries must apply graduated safeguards that are commensurate with the risks to their information and IT assets, with more rigorous safeguards as asset values, service delivery requirements and threats to confidentiality, availability or integrity increase.

Ministries can reduce overall security costs for IT systems by segregating sensitive information and services and focusing more expensive and restrictive safeguards on a limited array of assets.

IT Processes That Support Security
As a foundation for IT security, Ministries would apply the following general controls.

Configuration Management and Change Control
When proposing configuration management or system changes, Ministries must seek the advice of the IT Security Coordinator where changes could potentially compromise security.

Problem Reporting/Help Desk
IT security measures must be incorporated into the routine functions of the MDA's problem reporting process or centralized Help Desk facility. The Help Desk is typically the first point of contact for users to report issues such as password problems, data corruption, network performance issues, or service outages. Where the incident involves a possible security breach, documented response procedures must outline how Help Desk personnel will document the event, identify trends, notify the IT Security Coordinator or an incident response team, and instruct the user on how to proceed.

Capacity Planning

In support of availability requirements, Ministries should monitor system and network capacity in order to plan and implement timely capacity changes.

System Support Services
Ministries must ensure that underlying system services (e.g. trusted time, event logging) are provided to support security services.
Based on a trusted time source, Ministries provide an accurate time and date throughout their systems and networks. Trusted time is particularly important in activities as electronic financial transactions and digital signatures, and for audit and investigations.

Active Defense Strategy
Ministries must adopt an active defense strategy that includes prevention, detection, response and recovery (PDRR). Prevention is the first line of defense. Because prevention safeguards can be defeated, Ministries have to be able to detect incidents rapidly, respond quickly to contain damage, and recover systems and data in a timely manner.

Ministries must continuously monitor threats and vulnerabilities and, where required, take proactive countermeasures. Ministries must consider information from security vendors and external surveillance bodies. During increased Readiness Levels or periods of heightened IT threat, Ministries are required to increase their vigilance by, for example, increasing the operating hours of a MDA Information Protection Centre to twenty-four hours a day, seven days a week.

Ministries that have highly sensitive, critical information and IT assets or that depend on complex networks and systems may benefit from establishing a dedicated Information Protection Centre (IPC). An IPC would coordinate active defense within the MDA, and ensure the MDA communicates and cooperates with other security organizations.

Prevention
Prevention safeguards protect the confidentiality, integrity, and availability of information and IT assets.

Physical Security within the IT Security Environment
Physical security measures, e.g., locks and alarm systems, reduce the risk of unauthorized access to information and IT assets. Physical security can also protect information and IT assets from fire, floods, earthquakes, and power failure etc.

Ministries must protect portable devices such as laptops, handheld digital devices and cell phones, given the information they contain and their monetary value.
Ministries that need to destroy or dispose of IT media containing classified or protected information must follow the methods and procedures defined in associated technical documentation.

Storage, Disposal and Destruction of I.T Media
Ministries must mark IT media containing classified or protected information, and must:

- store backup or sensitive IT media, supporting high or medium availability systems or services, in containers designed to resist fire or other environmental damage (this applies to both on-site and off-site storage), and
- dispose of IT media containing classified or protected information

Personnel Security in the IT Security Environment

The purpose of personnel security measures is to establish trust in personnel and others, who require access to government systems and networks.

The security requirements for personnel screening apply to positions and contracts requiring access to information and assets relating to information technology and ITS. In addition, Ministries must screen all personnel with privileged access to critical systems.

Technical Safeguards

Selection of Security Products

Ministries should consider the cost, quality, effectiveness, ease-of-use, assurance, and impact on the performance of the MDA's systems when selecting security products. Ministries should use evaluated products, especially in systems where the security afforded by that product is assured.

Identification and Authentication

Ministries must incorporate identification and authentication safeguards in all their networks and systems, according to the level or risk for the network or system. When assigning a unique identifier for users, Ministries must ensure the proper identification of the individual to whom the identifier is issued.

Identification and authentication is important because most other security safeguards rely on it. For low-risk environments (e.g., access from an internal network, or systems with low sensitivity information), Ministries can use simple authentication methods (e.g., password) if passwords are well managed and protected. For higher risk environments (e.g., access from external networks such as the Internet, or systems with high sensitivity information), Ministries can use stronger authentication methods (e.g. cryptographic-based). If additional security is required, Ministries can use safeguards such as tokens or biometrics.

Authorization and Access Control

Ministries must restrict IT and information access to individuals who have been screened and authorized; have been identified and authenticated; and have a "need to know."

Ministries must keep access to the minimum required for individuals to perform their duties (i.e., the least-privilege principle), and ensure that they are regularly updated to accurately reflect the current responsibilities of the individual. Ministries must withdraw access privileges

from individuals (including students, contractors, or others with short-term access) who leave the organization, and revise access privileges when individuals move to jobs that don't require the same level of access.

Cryptography

When properly used, cryptography is an effective means of ensuring confidentiality, integrity, authentication and non-repudiation. Ministries must ensure effective key management, including the protection and recovery of cryptographic keys.

Ministries must use encryption or other safeguards to protect the electronic communication of classified information. Ministries should encrypt information, when supported by a Threat and Risk Assessment. However, Ministries must encrypt information before transmitting it across the Internet or a wireless network.

Public Key Infrastructure

Public Key Infrastructure (PKI) is one way that Ministries can fulfill requirements for authentication, confidentiality, integrity and non-repudiation. PKI provides public key encryption and digital signatures as well as processes for managing public keys.

Network Security and Perimeter Defense

Ministries must segregate networks into IT security zones and implement perimeter defense and network security safeguards. The use of I.T security zones by all Ministries ensures a consistent, minimum level of protection of data communication networks across the government.

Ministries must strictly control all Public Zone interfaces, including all external uncontrolled networks such as the Internet, at a defined security perimeter. Ministries must use perimeter defense safeguards (e.g. firewalls, routers) to mediate all traffic and to protect servers that are accessible from the Internet.

Mobile Computing and Teleworking

Off-site use of MDA I.T assets can introduce additional information security risks. Ministries that allow personnel to access MDA information and IT assets, networks and systems from outside their government offices must establish procedures for such use.

To protect the remote computer, the information it contains, and the communications link, Ministries should use an effective combination of physical protection measures, access controls, encryption, malicious code protection (e.g. virus scanners), backups, security configuration settings (e.g. operating system controls), identification and authentication safeguards, and network security controls (e.g. a PC firewall).

Ministries must ensure that personnel working off-site are made aware of their security responsibilities, including the sensitivity and criticality of the information and IT assets they access.

Wireless Devices

The use of wireless devices can introduce additional information security risks. Ministries must apply appropriate safeguards and restrict the use of such devices to individuals who have received MDA approval. Users must turn off wireless devices with a voice transmission capability when attending a meeting at which sensitive information, is being shared.

Emanations Security

Most electronic equipment radiates electromagnetic signals that, if intercepted, can compromise sensitive information. Two fundamental approaches to mitigating this risk are source suppression and containment of the information- bearing signals. Collectively, these safeguards are referred to as TEMPEST.

In Jamaica, Ministries should use TEMPEST protection for Top Secret information when justified by a Threat and Risk Assessment. At posts abroad, Ministries should apply TEMPEST protection to all classified information when justified by a Threat and Risk Assessment.

Telecommunications Cabling

Ministries need to protect telecommunications cabling from unauthorized interception and damage. Ministries must authorize, control and monitor access to telecommunications wiring, spaces and pathways (i.e., telecommunications rooms, main terminal rooms and other equipment rooms) in a manner appropriate for the sensitivity level of the information being transmitted.

Ministries should ensure additional protection, such as a Red Distribution System (RDS), for the transmission of classified information. Where physical security safeguards are impractical, Ministries should use encryption or other methods approved by the CIO.

Software Integrity and Security Configuration

Safeguards to prevent and detect the integrity of software can help to avoid many potential security incidents.

Ministries should configure their operating systems and application software in accordance with security best practices. Ministries must configure their systems to control the use of mobile code (e.g. Javascript).

Ministries must implement safeguards to "harden" software that is exposed to the Internet (e.g. Web servers and their software) or servers supporting sensitive applications. At a minimum, Ministries should remove or disable unnecessary services and applications and properly configure user authentication.

Ministries should prohibit the use of unauthorized software, and should have a capability to scan networks to detect unauthorized software.

Malicious Code

IT systems are vulnerable to malicious code such as viruses, Trojan horses, and network worms. E-mail file attachments are among the most common sources of malicious code.

Ministries must install, use and regularly update antivirus software and conduct malicious code scans on all electronic files from external systems. Ministries must install new virus definitions as soon as practical. Ministries should implement antivirus detection software at several points in the infrastructure including desktop computers, servers, and MDA entry points.

Detection

To detect incidents, Ministries can, subject to applicable laws and relevant policies, use firewalls and routers, audit logs, virus and malicious code detection software, system performance tools, health-monitoring tools, integrity checkers, and host- and network-based intrusion detection systems. The rigor and extent of detection will depend on the level of risk, including the sensitivity (in terms of confidentiality, availability and integrity) and the system exposure.

To protect information and ensure service delivery Ministries must continuously monitor system performance to rapidly detect:

1. attempts (failed or successful) to gain unauthorized access to a system, or to bypass security mechanisms unauthorized probes or scans to identify system vulnerabilities
2. unplanned disruption of systems or services
3. denial-of-service attacks
4. unauthorized changes to system hardware, firmware, or software
5. system performance anomalies, and
6. known attack signatures.

At a minimum, Ministries must include a security audit log function in all IT systems. Ministries must incorporate automated, real-time, incident detection tools in high risk systems.

Response and Recovery

Incident Response Coordination

Ministries should be required to establish mechanisms to respond effectively to IT incidents and exchange incident-related information with designated lead Ministries in a timely fashion. To do so, Ministries must appoint an individual or establish a center to coordinate incident response and act as a point of contact for communication with respect to government-wide incident response. Ministries that do not have an Information Protection Centre should assign this function to the IT Security Coordinator.

The Government of Jamaica systems and networks should be viewed as a single interconnected entity that requires a coordinated incident response. The office of the CIO must be responsible for coordinating incident response across the central government and, with other lead agencies, providing technical assistance, advice and information on the handling of IT security incidents.

Incident handling generally follows five stages:

1. Identification - determine the type, severity and cause of the incident(s) (e.g. virus, worm, denial-of-service-attack),
2. Response - determine the best approach and take action to contain the damage (e.g. disconnect, disable, block, or update computer or network configurations),
3. Reporting - communicate the incident specifics, including the impact and the response, to MDA management,
4. Recovery - identify an approach to restore and recover systems and implement approved changes to security devices (e.g. firewall and incident detection rules), and
5. Post-Analysis - Assess the incident and recommend changes in processes and procedures, if required.

Incident Identification and Prioritization

If monitoring reveals an anomaly, Ministries must determine whether the cause is a security incident, a hardware or software problem, or an increase in client demand. An IT security incident refers to an adverse event in an information system or network or the threat of the occurrence of such an event. Incidents can include but are not limited to:

- Denial of Service (DoS) - an attack that could prevent the usage of networks, systems, or applications,
- Malicious Code - a virus, worm, Trojan horse, or other code-based malicious entity that infects a host,
- Unauthorized Access - a user who gains access without permission to a network, system, applications, data, or other resource, and
- Multiple Impacts - a combination of a number of computer events occurring at the same time or a computer event in coordination with other malicious or accident incidents.

To analyze IT security incidents effectively, Ministries must understand the types of IT security incidents that can occur, their potential impact, the technical and operational environment, and service delivery priorities.

Typically this analysis involves the following steps:

- Determine if an incident has occurred
- Perform an assessment of the severity of impact or potential impact
- Identify the type, cause, and source
- Log the event

If more than one incident occurs at the same time or is too complex, Ministries should prioritize and focus on the most significant incident event first. Factors to consider include risks related /to:

- Human life and safety,
- Valuable, sensitive and critical information and assets,
- Disruption to operations or services, and
- Public confidence

Incident Response

Ministries must develop incident response procedures to follow in order to mitigate damage, contain the cause of the incidents and restore services.

Given the interconnectivity of the Government of Jamaica, Ministries must always, when responding to an IT security incident, consider the impact of their actions or inaction on other organizations, ministries, departments.

Ministries must maintain operational records that show how incidents were handled, documenting the chain of events during the incident, noting the time when the incident was detected; the actions taken; the rationale for decisions; details of communications; management approvals or direction; and external and internal reports.

Incident Reporting

Ministries are required to establish an internal and external incident reporting process. To meet these requirements, Ministries must

- report incidents and threats to, and share information, subject to applicable legislation and relevant policies, about the incidents and the effectiveness of their response,
- participate in threat and risk briefings and teleconferences,
- establish a procedure for notifying the appropriate operational personnel, managers and all affected parties, keeping contact lists up to date. (e.g., The IT Security Coordinator, the MDA Security Officer, the Chief Information Officer, business or system managers),
- notify the appropriate law enforcement agency if the incident appears to be criminal and the security forces e if the incident has national security implications.

Where required, Ministries will be assisted by the relevant agencies in determining the nature of the incident. Legal advisors should be consulted where there is suspicion of criminal activity.

In the event that the established primary means of communications is not available, Ministries should establish an alternative means to communicate incident related information.

Recovery

Before reconnecting or restoring services, Ministries must ensure that all malicious software has been removed and that there is no potential for recurrence or spread.

Ministries must restore essential capabilities within the time constraints and the availability requirements.

To be able to recover information, Ministries must

- back up data regularly
- test backups regularly to ensure that they can be used for recovery
- back up all software and configuration data
- facilitate the restoration of data and services by allowing systems to undo operations and return to an earlier state (e.g., rollback services)

- test restoration procedures regularly to ensure that they are effective and that they can be completed within the time allotted for recovery
- determine retention periods for essential business information and archived backups, and
- document, in a memorandum of understanding or other agreement, all arrangements for off-site backup (in case the off-site backup is with another party).

Note that system recovery should be conducted in a manner that preserves the integrity of evidence, in the event of a criminal investigation of a security breach, for example.
Ministries may seek support and advice for this process from the CIO.

Post-Incident Analysis
For every severe or major IT security incident that occurs, Ministries must perform a post-incident analysis which summarizes the impact of the incident, including cost, and identifies

- security deficiencies,
- measures to prevent a similar incident,
- measures to reduce the impact of a recurrence, and
- improvements to incident-handling procedures.

When requested by the CIO, Ministries must share the lessons they learn from their post-incident analysis. By sharing such information across the government, Ministries can learn from the analyses of other Ministries and lead agencies.
Ministries should periodically analyze their own security incident statistics to identify recurring problems or patterns of attack and to estimate the overall cost of incidents with a view to improving service delivery.

Enquiries

The ICT Council is responsible for the policy instruments supporting this policy framework; please direct any enquiries to:

Chief Information Officer

Office of the CIO

(876) 929-8990 - 9
(876) 960-1623
cio@mset.gov.jm

11. Glossary of Terms

Compromise
unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

Critical asset
assets supporting a critical service.

Critical service
service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the efficient functioning of the Government of Canada.

Government information
information created, received, used, and maintained regardless of physical form, and information prepared for or produced by the Government of Canada and deemed to be under its control in the conduct of government activities or in pursuance of legal obligations.

Graduated safeguards
A set of increasingly secure safeguards that respectively reduce risk.

Intrusion
a type of IT security incident involving unauthorized access to, or activity on, a system or network.

Intrusion Detection System (IDS)
software that looks for suspicious activity and alerts administrators.

Information Technology (IT) Security
safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

IT Security incident
any unexpected or unwanted event that might cause a compromise of business activities or information security.

IT Security Zones
a networking environment with a well-defined boundary, a security authority and a standard level of susceptibility to network threats.

Patch management
a component of change management, involving the acquiring, testing, and installing of software fixes on an administered IT system.

Risk management
a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.

Security risk management
a component of an overall risk management process involving the organization and coordination of activities and processes for controlling security risk.

Service
a collection of one or more systems that perform a useful function in support of business direction.

Software integrity
the process of developing software with minimal vulnerabilities.

System
A set of elements such as personnel, physical, environment, safeguards, technology, etc. that are combined together to fulfill a specified purpose or mission.

Vulnerability
an inadequacy related to security that could permit a threat to cause injury.

Vulnerability assessment
a determination of the existence of system vulnerabilities.

12. Guidelines

- Guidelines for Secure Connections Across Web Sites and Services
- Guidelines for Official Use of Social Media
- Guidelines for GoJ Cloud Computing

This Page Intentionally Left Blank

Guidelines for Secure Connections Across Web Sites & Services

1. Background Information

The Government of Jamaica (GoJ) is the largest repository of data on and about its citizens. The majority of GoJ websites use HTTP as the as primary protocol to communicate over the public internet. Unencrypted HTTP connections create a privacy vulnerability and expose potentially sensitive information about users of unencrypted government websites and services. The unencrypted HTTP protocol does not protect data from interception or alteration, which can subject users to impersonation, eavesdropping, tracking, and the modification of received data. This data can include browser identity, website content, search terms, and other user-submitted information.

To address these concerns and keep pace with privacy and security practices used globally as well as to protect visitors to our websites and services, **it is required that all publicly accessible GoJ websites and web services only provide service through a secure connection**. This will provide the public with a consistent, private browsing experience and position the GoJ as a leader in Internet security. The strongest privacy and integrity protection currently available for public web connections is HTTPS. An HTTPS-Only standard will eliminate inconsistent, subjective determinations across ministries, departments, and agencies regarding which content or browsing activity is sensitive in nature, and create a stronger privacy standard government-wide.

2. Definitions

Term	Definition
GoJ	Government of Jamaica
HSTS	HTTP Strict Transport Security. It forces all responses to pass through HTTPS connections instead of plain text HTTP ensuring that the entire channel is encrypted before being sent.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol.
Intranet	For these guidelines and related documents, an intranet is a computer network that is not directly reachable over the public internet.
MDA	Ministry, Department and Agency /Ministries, Departments and Agencies
PPC	Programme Portfolio Committee of the ICT Council
SPDY Protocol	A deprecated open source TCP based, application layer protocol developed by Google's Chromium group primarily geared towards reducing web page latency.

Term	Definition
TLS	TLS is an authentication and security protocol widely implemented in browsers and Web servers that establishes an encrypted connection to an authenticated peer over an untrusted network.

3. Scope

These guidelines are applicable to all **GoJ ministries, departments and agencies'** staff and their associates, all users of ICT equipment owned or leased by the institution as well as all equipment connected to each MDA's ICT related infrastructure. These guidelines relate to all MDAs' ICT related resources and services.

4. Guideline Statement

In order to promote the efficient and effective deployment of HTTPS, the timeframe for compliance, outlined below, is both reasonable and practical. These guidelines require that all government agencies deploy HTTPS on their domains using the following guidelines.

- Newly developed websites and services at all GoJ agency domains or subdomains should adhere to these guidelines and related policies upon launch.
- For existing websites and services, agencies should prioritize deployment using a risk-based analysis. Web services that involve an exchange of personally identifiable information (PII), where the content is unambiguously sensitive in nature, or where the content receives a high-level of traffic should receive priority and migrate as soon as possible.
- MDAs should make all existing websites and services accessible through a secure connection (HTTPS-only, with HSTS) by **March 31, 2018**. Any MDA not able to be compliant ny the stated date, as may be the case for entities experiencing issues in respect of acquisition of security certificates, should request of the Office of the CIO an extension of the timeframe, providing justification for this.
- The use of HTTPS is strongly encouraged on corporate intranets, but not explicitly required.

Considerations

APIs and Services	• Web services that serve primarily non-browser clients, such as web APIs, may require a more gradual and hands-on migration strategy, as not all clients can be expected to be configured for HTTPS connections or to successfully follow redirects.
Mixed Content	• Websites served over HTTPS need to ensure that all external resources (images, scripts, fonts, iframes, etc.) are also loaded over a secure connection. • Modern browsers will refuse to load many insecure resources referenced from within a secure website. • The migration of existing websites can involve a combination of automated and manual effort to update, replace, or remove references to insecure resources which, for some websites can be the most time consuming aspect of the migration process.
Planning for Change	• Protocols and web standards improve regularly, and security vulnerabilities can emerge that require prompt attention. Federal GoJ websites and services should deploy HTTPS in a manner that allows for rapid updates to certificates, cipher choices.
Server name indication	• The Server Name Indication extension to TLS allows for more efficient use of IP addresses when serving multiple domains. However, these technologies are not supported by some legacy clients. Web service owners should evaluate the feasibility of using this technology to improve performance and efficiency.
Site performance	• While encryption adds some computational overhead, modern software and hardware can handle this overhead without substantial damaging or harmful impact on server performance or latency. Websites with content delivery networks or server software that supports the SPDY or HTTP/2 protocols, which require HTTPS in some major browsers, may find their site performance substantially improved as a result of migrating to HTTPS.
Strict Transport Security	• Websites and services available over HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS going forward. This reduces the number of insecure redirects, and protects users against attacks that attempt to downgrade connections to plain HTTP. Once HSTS is in place, domains can be submitted to a "preload list" used by all major browsers to ensure the HSTS policy is in effect at all times.

Cost Effective Implementation

Implementing an HTTPS-only standard does not come without a cost. A number of GoJ websites have already deployed HTTPS. The goal of these guidelines is to mandate the adoption of HTTPS throughout the GoJ.

5. Distribution/Communication

The PPMC's Policy, Standards and Guidelines Subcommittee will ensure that:

1. all stakeholders receive a copy of these guidelines during the induction process
2. these guidelines are easily accessible by all stakeholders
3. stakeholders are informed when a particular activity aligns with these guidelines
4. stakeholders are empowered to actively contribute and provide feedback to these guidelines
5. stakeholders are notified of all changes to these guidelines

6. Monitoring and Review

The PPMC's Policy, Standards and Guidelines Subcommittee will review this policy six months after implementation and annually thereafter. Effectiveness of the guidelines will be assessed through:

6. feedback from stakeholders
7. review of the guidelines and related documents by the Sub-Committee to determine if objectives have been met.

7. Related Information

These guidelines will be subsumed within a web security policy and may also be referenced in any future data protection legislation.

8. Guideline History

This is the first version of these guidelines and as such contains no amendments.

9. Technical Assistance

The ICT Council is responsible for the policy instruments supporting this Policy Framework; please direct any enquiries to

Chief Information Officer

Office of the CIO

(876) 929-8990 - 9

(876) 960-1623

cio@mset.gov.jm

10. Appendices

HTTPS Dos and Don't

HTTPs does/is designed to	HTTPS doesn't/not designed to
• Verify the identity of a website or web service for a connecting client, and encrypt nearly all information sent between the website or service and the user.	• Encrypt IP addresses and destination domain names during communication.
• Facilitate browsers and other HTTPS clients be configured to trust a set of certificate authorities that can issue cryptographically signed certificates on behalf of web service owners.	• Protect a web server from being hacked or compromised, or to prevent the web service from exposing user information during its normal operation.
• Guarantee the integrity of the connection between two systems, not the systems themselves.	

Guidelines

Secure Connections across GoJ Websites and Web Services

VERSION: 1.00	REVISION DATE:

This document is based on the work of the Policies, Standards and Guidelines Subcommittee of the Program Portfolio Committee of the ICT Council and its working groups.

Approval Form/ Signature(s)

Decision:

- ☐ Approved and execution is authorized
- ☐ Approved, but deferred until further notice
- ☐ To be revised and resubmitted for approval
- ☐ Rejected

[NAME	[NAME
[TITLE]	[TITLE]
DATE	DATE

The signatures of the people above relay an understanding in the purpose and content of this document by those signing it. By signing this document you agree to this as the formal Secure Connections across GoJ Websites and Web Services Guidelines.

Revision History

1.	Ver. 1.0	2017-06-06	PPC's PSG SubCommittee	Document created
2.	Ver. 1.0			Document approved

Guidelines for Official Use of Social Media

About This Guideline

The *Guideline on Official Use of Social Media* provides MDA managers and functional specialists responsible for official social media accounts with guidance on implementing the *Standard on Social Media Account Management* (the Standard).

This guideline was prepared by the Office of the Chief Information Officer, Jamaica. It supports the Government of Jamaica's renewed thrust of revolutionizing the ways in which it communicates with its citizens in the virtual space.

1. Introduction

The type of effective communication that the Government of Jamaica envisions, requires that government ministries employ a variety of ways and means to communicate and provide information in multiple formats to accommodate diverse needs. It also supports the use of all means of communication, from traditional methods to new technologies, in order to reach and communicate with Jamaicans wherever they may reside. Accordingly, the Government of Jamaica encourages the use of social media in communicating and engaging with the public and in delivering services.

This guideline defines official use of social media and presents the key policy and legal requirements for ministries to consider when using social media for official purposes. In particular, this document provides practical advice and tools related to the following:

- Preparing a ministerial social media strategy;
- Developing social media implementation plans;
- Assessing the risks of using third-party social media platforms, and developing a risk management plan;
- Developing a performance measurement plan;
- Requesting the creation, configuration and disposition of official accounts; and
- Using the Government of Jamaica social media platform management tool.

2. What is Official Use of Social Media?

There are important differences between official use of social media and other types of use. The advice provided in this guideline applies to official use of social media only.

Official Use

Official use of social media refers to the use of an official social media account on behalf of the Government of Jamaica. Only those individuals who have been authorized to represent the Government of Jamaica can use official social media accounts. Uses can include publishing messages, uploading content (e.g., text, images, audio, video), and responding to communications.

An official social media account is an account on a social media platform that is used for official Government of Jamaica purposes such as communication, service delivery, collaboration and other purposes within the scope of a department's mandate, including as a designated spokesperson for the department.

Other Uses

While social media is also used for professional and personal reasons, these uses are not covered by this guideline.

Professional use refers to the use of a personal social media account for purposes related to professional activities, such as communicating with professional associations, professional networking (e.g., participating in an online conference), knowledge gathering and sharing (e.g., using Twitter to stay up-to-date on trends, visiting government Facebook pages), and career development (e.g., maintaining a LinkedIn profile).

Personal use refers to the use of a personal social media account for purposes unrelated to professional development or employment (e.g., blogging about gardening tips, sharing personal or family photos).

Note: For advice on professional and personal use, please consult the *Guideline on Acceptable Network and Device Use*.

3. Policy and Legal Considerations

In the central government, various policy and legal requirements apply to the official use of social media. Meeting these requirements requires knowledge and understanding of relevant legislation and policies, proper planning, ongoing monitoring of the official social media account, and long-term evaluation and improvement.

In preparing for an official social media account, it is a good practice to consult with the appropriate ministerial representatives in the following key areas to ensure that the necessary policy and legal requirements are met:

- Accessibility;
- Communications;
- Federal Identity Program;
- Information management;

- Information technology security;
- Legal services;
- Privacy and access to information; and
- Values and ethics.

When seeking advice, it is a good idea to provide information on the proposed use of the official account, the functionality of the platform and its terms of use.

Appendix A offers further guidance on the key policy and legal areas that apply to the official use of social media.

4. **Implementing the Standard on Social Media Management**

The objective of the Standard is to enable a strategic and coherent approach to the management of official Government of Jamaica social media accounts. The expected results are official social media accounts that are clearly identified as belonging to the Government of Jamaica; that are effectively managed within Ministries and government-wide; and that enhance opportunities for communication, collaboration and service delivery.

The following are the responsibilities of ministerial heads of communications or designates:

- Approving an overarching ministerialsocial media strategy;
- Approving official social media accounts based on implementation plans, and overseeing the life cycle of official social media accounts, including planning, creation, configuration, implementation, evaluation and disposition;
- Providing submissions related to the creation, configuration and disposition of official social media accounts to the entity for review;
- Ensuring that ministries use the Government of Jamaica social media platform management tool to manage official social media accounts as prescribed by the entity; and
- Ensuring that official social media accounts meet the layout and design specifications outlined.

This section of the guideline provides advice on implementing the Standard.

4.1 Ministerial Social Media Strategy

A social media strategy provides the foundation for guiding the social media activities of a ministry. It explains how the official use of social media supports the ministerial mandate and program objectives. It also provides the ministry with a clear rationale and intended outcomes for using social media platforms.

Without this strategic direction, a ministry may risk creating unsustainable and inadequately resourced efforts to maintain an effective social media presence. This can result in efforts that detract from the ministry's mandate and objectives, rather than promote them.

The head of communications or designate is responsible for approving the ministerial social media strategy. It is recommended that this strategy be updated on an annual basis.

Key Elements of a Social Media Strategy

The recommended elements of a ministerial social media strategy are:

- **Overview** of the ministry's social media presence to date, if any, and the context in which it takes place from both an overall Government of Jamaica perspective and the perspective of the department.
- **Business value and objectives** of engaging with Jamaicans on social media platforms and how these objectives relate to the ministerial mandate. A clear articulation of this element will enable measurement of the strategy's success, once it is implemented.
- **Governance and resources** allocated to official social media activities, including the identification of a **ministerial coordinator** for official social media accounts. It is recommended that ministries leverage existing resources and governance structures within the ministry, whenever possible. It is a good practice to have clear, succinct and well communicated governance processes so that everyone is aware of their respective responsibilities for official use of social media, and how decisions are made.
- **Strategic approach** to using social media platforms in line with the ministry's mandate and objectives. Use of social media platforms is usually done on a priority basis, beginning with the most popular and effective platforms for the ministry's social media objectives and target audiences. In some cases, it is useful to identify the strategic direction and objectives for each major platform.
- **Criteria and tools to define and measure the strategy's success** and the effectiveness of its approach to meeting the stated objectives.
- How to **integrate lessons learned** and support continuous improvement.

Appendix B provides a sample template for developing and updating a social media strategy.

4.2 Social Media Implementation Plans

Implementation plans are based on the ministerial social media strategy. Their objective is to ensure that the key factors for properly establishing and managing official social media accounts are considered during the implementation process. The head of communications or designate approves the social media implementation plans as well as the accounts, based on those implementation plans.

A recommended practice is to prepare an implementation plan for each official social media account or related group of accounts, including the accounts that already exist. This is particularly important if the ministry has more than one account on the same platform (e.g., a corporate account and a program account). Each implementation plan articulates the proposed use of each official social media account.

It is a good idea to engage the ministerial coordinator for official social media accounts during the development of the implementation plans and to review and update these plans regularly.

Key Elements of a Social Media Implementation Plan

The following presents the recommended elements of a social media implementation plan. Appendix C provides a sample template to use in developing an implementation plan.

a) Objectives and Business Drivers

This element outlines how the official social media account aligns with the ministerial social media strategy, and articulates the rationale and the objectives that it aims to achieve. Important questions to answer in this section include the following:

How does this account support the ministerial mandate and social media strategy?
What are the business drivers and objectives of this account?
What are the proposed uses of this account?

b) Choice of Platform

This element describes the key considerations in choosing a social media platform.

An important consideration is the target audience. A social media scan can help determine which platform is best suited to the target audience. The scan investigates who (target audience), what (message), where (which social media platform), when (when there is most activity) and why (strategic reasoning) people are engaging around subjects that are directly or indirectly related to the ministerial mandate and objectives.

It is also useful to understand the features and functionality of the platform and how the target audience will use them.

Other important considerations in choosing a platform include:

- What accessibility options and alternative means of accessing the platform are available;
- What terms of use apply, and whether there are any policy or legal compliance issues (discussed in Section 3 of this guideline).

c) Allocation of Resources

This element identifies the human and financial resources that will be assigned to manage the official social media account according to its planned use. It is a good practice to include resources for training staff on the official use of social media and the platform, and for ensuring knowledge transfer and continuity as technology changes.

d) Delineation of Roles and Responsibilities

This element identifies the roles and responsibilities of those who will be involved in using and managing the official social media account. Rather than identifying specific individuals, it is useful to identify the ministerial areas responsible for the key functions such as drafting, translating, approving and publishing content; administering and monitoring the account; and managing account issues, should they arise.

e) Risk Management Plan

This element involves identifying and assessing the risks associated with the proposed use of the official social media account in relation to the ministerial mandate. It also involves identifying strategies to manage those risks.

There are numerous tools and techniques for ministries to identify, analyze and mitigate risks, depending on the context. Ministries are encouraged to design the risk management process and tools that are appropriate for their own operating environment (e.g., threat and risk assessments, business impact analysis, privacy impact assessments, self-assessments, statements of sensitivity, vulnerability assessments).

Following are examples of risks that would need to be identified, assessed and mitigated. Note that this is not an exhaustive list; each risk management plan needs to thoroughly identify and assess the risks associated with the use of each official social media account:

- Risks related to **policy and legal obligations** that may arise from using the platform and/or accepting its terms of use (see Section 3 of this guideline);
- Risks related to the **functionality** of the platform regarding Government of Jamaica policy and legal requirements, such as privacy, accessibility and intellectual property (including copyright);
- Risks related to the **security** of the official social media account, such as potential hacking and vandalism of content;
- Risks related to the **actual use** of the official social media account, such as communications and reputational risks (e.g., unintentional errors, criticism for not meeting user expectations regarding response time, usefulness of content, language, tone);
- Risks related to the **use of a third-party platform**, including lack of availability (e.g., platform is over capacity or down for maintenance) changes to the platform and inappropriate content appearing on the same page as the official account's content; and
- Risks related to the **management of the account**, such as lack of resources to manage and monitor the account properly and an unexpected amount of direct communication due to unforeseen developments.

f) Government of Jamaica Privacy Impact Assessment and Threat and Risk Assessment

A Privacy Impact Assessment (PIA) and Threat and Risk Assessment (TRA) are integral components of a social media risk management plan. The PIA and the TRA assess, respectively, the privacy and security risks that are associated with the official social media account's proposed uses on the selected social media platform.

To help ministries prepare their social media risk management plans, the entity will pre-review platforms used by the Government of Jamaica. These pre-reviews will cover the platform's functionality and terms of use, and will include privacy and security risk assessments from a government-wide perspective. Specifically, the entity will prepare a Government of Jamaica (enterprise) PIA and TRA for the most frequently used social media platforms.

If the ministry's proposed uses of the platform are similar to the uses identified in the Government of Jamaica PIA and TRA for social media, then the department can leverage the Government of Jamaica PIA and TRA.

When a ministry's proposed use of a platform is different from the uses assessed by the Government of Jamaica PIA and TRA, or if the platform has not been pre-reviewed by the entity, it is recommended that the department carry out its own risk assessments (e.g., functionality, terms of use, privacy and security) and that those assessments be shared with the entity so that they can be leveraged by other departments. The department will also need to keep their assessments up to date whenever there are changes to the platform in question.

It is important to consult with legal counsel, communications advisors, social media functional specialists, the ministerial coordinator for official social media accounts and other ministerial representatives listed in Section 3 of this guideline to determine whether the entity's pre-reviews and the Government of Jamaica PIA and TRA can be leveraged, or whether separate assessments of risks need to be conducted.

The entity will maintain a list of pre-reviewed platforms and will keep it up to date whenever there are platform changes (for example, if the privacy policy or the terms of use of the platform change). Only accounts on platforms that have been pre-reviewed by the entity will be included in the index of official Government of Jamaica social media accounts, which will be maintained and published by the entity.

g) Management Protocols

This element describes the internal processes that will ensure effective, open and transparent engagement practices for managing an official social media account. Ministries may wish to establish management protocols for each social media platform, rather than individual protocols for each account.

Management protocols for moderation, engagement and interaction, and content are recommended, as well as a plan for dealing with contentious issues that may arise. It is important to keep in mind the protocols required to meet the social media notice requirements in Appendix C of the *Standard on Web Usability*, as described in subsection 4.5 of this guideline

h) Performance Measurement Approach

This element describes the method and tactics used to determine whether the official social media account is being used effectively to meet its stated objectives. Generally, the performance measurement of an official social media account is linked to the overall performance measurement objectives and the approach of the ministerial social media strategy. It may also be linked to other established ministerial performance measures.

Based on the objectives of the account and strategy, performance measurement may involve specific and quantifiable metrics (e.g., number of followers, posts, re-tweets, replies, direct messages) or a more qualitative approach (e.g., tone and quality of comments and video replies). It is a good practice to establish a process to report and leverage the performance measurement outcomes on an ongoing basis to improve the official use of social media.

Appendix D provides a sample template for performance measurement.

i) Communications Plan

This element helps align messages communicated through the official social media account with messages delivered through other ministerial communication channels and activities. It is important to consult with the ministerial communications advisor on the development of this element.

j) Phasing Out Accounts

This element describes the exit strategy to determine when and how to shut down an official social media account (i.e., the conditions that would prescribe an official social media account to be closed). Short-term accounts are discouraged due to the amount of time and effort required to establish a solid social media presence and reputation, and build up followers. In most cases, a combination of the proper use of tags, links and targeted messaging is likely to serve the purposes of a short-term account.

It is important to plan how and why an account will be phased out. For example, an official social media account may be closed when, despite corrective measures, the account is not seen to be meeting its stated objectives. It is a good idea to advise followers of the situation in advance, via the account, providing reasons for closure and options for further communication.

4.3 Creation, Configuration and Disposition of Accounts

Once the social media implementation plan is complete and the ministerial head of communications or designate has approved the official social media account, the ministerial coordinator for official social media accounts provides the entity with a submission for the creation and configuration of the account. After reviewing the submission and providing feedback as needed, the entity will create and configure the official social media account on behalf of the ministry, based on the information provided in the request template. As part of the creation of the account, the entity will provide user information details to the platform provider and will accept the terms of service and related conditions on the ministry's behalf.

The entity will configure the account in a manner that meets the official layout and design specifications and that maximizes privacy, security and usability considerations. Configuration will also be done in a manner that enables the use of the Government of Jamaica social media platform management tool (see subsection 4.4 of this guideline).

Note: Ministries that are not using a pre-reviewed platform still need to provide a submission and work with the entity on the creation and configuration of the account.

The entity will also review submissions related to the disposition of official social media accounts.

4.4 Social Media Platform Management Tool

The Government of Jamaica social media platform management tool will be provided and administered by the entity. This tool will give ministerial users direct access to their official social media accounts across different platforms through a single interface.

The entity will associate official social media accounts to the platform management tool. Ministerial users authorized in the submission template will be provided access to their accounts through the platform management tool.

4.5 Official Layout and Design Specifications and Social Media Notices

Official layout and design specifications provide the common Government of Jamaica approach to ensuring the proper identification of official social media accounts, including identification elements for official Government of Jamaica symbols and other images and graphic elements, as well as account usernames and addresses. The specifications also ensure that terms of use and privacy notices are available on all official social media accounts.

Social Media Notices

A social media notice informs users of their rights and obligations when interacting with the Government of Jamaica via social media. It also explains what users are to expect from official Government of Jamaica social media accounts. It is important to apply the social media notice to all official social media accounts through a hyperlink to the Terms and Conditions section of the associated Government of Jamaica website and, where possible, by incorporating the notice text within the profile of the official social media account.

In addition, Appendix D of the *Standard on Web Usability* states that where third-party icons are displayed to facilitate the sharing of content via social media, Ministries must provide a disclaimer indicating that no endorsement is implied or expressed.

5. Conclusion

The Government of Jamaica supports the official use of social media as part of the various channels available for communicating and engaging with Jamaicans. Through social media, government ministries can effectively reach people digitally where they reside, work, learn and play, and in this way enhance the opportunities for communication, collaboration and service delivery.

To maximize these opportunities, it is crucial that ministries manage their accounts strategically and coherently. This involves setting strategic social media direction, carefully planning and monitoring the implementation of each account and measuring performance.

Given the rapidly evolving nature of social media, quick access to up-to-date information on social media account management is important. Government of Jamaica social media practitioners and communities regularly develop and share lessons learned and good practices on the official use of social media.

Appendices

Appendix A: Key Policy and Legal Considerations

When using social media for official purposes, it is important to be aware of the policy and legal requirements that apply to the Government of Jamaica. To ensure that these requirements are met, it is a good practice to refer to original legislative and policy instruments and to consult with **legal services**, **communications advisors** and the appropriate ministerial **policy centres**. In seeking advice, it's best to provide information on the proposed use of the account, the functionality of the platform and its terms of use.

Legislative instruments that are likely to apply include the *Access to Information Act*; the *Jamaican Fundamental Rights Act*; the *Privacy Act*; In addition, there are other legal obligations such as intellectual property (including copyright), procurement, indemnity, Crown liability, ministerial policies and governing law.

Following is further discussion of the key policy and legal areas, presented in alphabetical order.

Accessibility

Government of Jamaica websites and web applications are the central government's primary means of delivering official information and services online. Social media platforms are used to supplement these means of delivery.

Before using a third-party social media platform, review the degree to which the platform is accessible and use the options provided by the platform to make the content more accessible. It is also recommended to provide a link to another online source that presents equivalent content at a high-level of accessibility.

Third-party sites generally have features that enhance the accessibility of web content, including the following:

- Text equivalents for non-text content (e.g., captions for images, transcripts for audio and video, and audible cues) so that all users can understand what is being presented; and
- Colour contrast to help users with colour vision deficiencies to distinguish between text and background or other types of text.

Communications

When using an official social media account to communicate or consult with the public, keep in mind that you are acting as a designated spokesperson according to the *Telcommunications of the Government of Jamaica*, and that the requirements of that policy apply.

Ministerial heads of communications are responsible for ensuring that:

- Official social media activities that are undertaken jointly with another government, company, organization, group or individual clearly and equitably identify the participation of all parties;
- Official social media activities that are undertaken to conduct public opinion research comply with the mandatory requirements of the Government of Jamaica;
- Official social media advertising activities comply with mandatory requirements; and
- Measures are taken to avoid conflicts of interest and the appearance or public perception of endorsing or providing a marketing subsidy or an unfair competitive advantage to any person, organization or entity outside of government.

For additional guidance, please contact the ministerial communications advisor.

Identity Program

Clearly identifying Government of Jamaica official social media accounts on third-party platforms and applying the government's corporate identity can present challenges. Page layouts and proprietary design controls often limit the size and display of visual elements, as well as the length of account names.

The *Technical Specifications for Social Media Accounts* should be developed to ensure a common approach to identifying the Government of Jamaica on all social media platforms, while taking into account these challenges and the evolving nature of government's use of these tools.

Information Management

The integration of information management requirements into official social media use is essential to ensure that digital information resources of value remain accessible, shareable and usable over time.

Most information posted on social media platforms represents information that has already been captured in official documentation (e.g., ministerial websites, briefing notes, project or communication plans). As such, the information used in social media, when otherwise captured through official documentation, is transitory and can be disposed of accordingly.

If a decision is made or an action taken via an electronic conversation on social media, the decision or action must be documented to ensure that the information is captured within the ministerial corporate

repository. Information on government programs and services distributed to Jamaicans should be captured in an official record in the ministerial corporate repository, regardless of format.

Examples of information resources associated with official use of social media that **are required** to be captured as a record in a ministerial information repository include:

- Official information made available through external social media platforms that has not otherwise been captured through official documentation such as ministerial websites, briefing notes, project or communication plans; and
- Information received from the public via external social media platforms in response to requests for information from Government of Jamaica ministries.

Examples of information resources that are **not required** to be captured in ministerial information repositories as a record include:

- Information, messages or official pages posted on social media platforms that have already been captured in official documentation (e.g., ministerial websites, briefing notes, project or communications plans); and
- Information in the form of electronic conversations that have taken place through the direct messaging components of external social media platforms (unless a decision or action is taken via the electronic conversation on social media, as described above, in which case the decision, action or rationale must be documented and captured within the ministerial corporate repository).

Information Technology Security

Following are a number of recommended actions to help ensure the secure use of social media, which are based on the requirements in the *Standard for Operational Security*. Many of these actions form part of the social media implementation plan's risk management approach, described in this guideline.

Recommended security actions include:

- Assessing and documenting the sensitivity of information that will be transmitted, stored and processed using social media platforms. Remember that all information made available through external-facing social media needs to be appropriate for release to the public at large.
- Ensuring that any unique risks to information, information technology assets and service delivery associated with the use of social media platforms are assessed, documented and understood, and that residual risks are accepted by program or service delivery managers.
- Formally documenting roles and responsibilities of personnel who will engage in the use of social media platforms.
- Ensuring that appropriate authentication and integrity controls are in place to prevent unauthorized account access.

- Ensuring that, where applicable and appropriate, information-sharing agreements are established and respected.
- Ensuring that, where applicable, incident management procedures have provisions to address incidents relating to, or resulting from, the use of social media platforms.
- Ensuring that employees who will be using social media platforms are provided with appropriate training on information technology security and information classification.

Privacy and Access to Information

Government institutions must respect privacy requirements when they engage in social media platforms. In particular, institutions that collect personal information on social media platforms, such as an individual's name, email address or Internet protocol address, must ensure that they have the legislative authority to do so, and that they collect the minimum personal information necessary to meet their legislated requirements.

The third-party social media privacy notice needs to reflect the legislative authority and the name and number of the Personal Information Bank (PIB) used. Institutions also have obligations regarding the use, disclosure, retention and disposal of personal information when they engage in social media platforms.

As discussed in subsection 4.2(f) of this guideline, a completed Privacy Impact Assessment (PIA) for the proposed uses of each official social media account is part of an institution's implementation plan. The completed PIA provides an overview of the privacy risks and mitigation strategies to ensure compliance with the Privacy laws of Jamaica. Ministries will be able to leverage the Government of Jamaica PIA if their proposed uses of the platform are similar to the uses that are identified in the Government of Jamaica PIA.

Values and Ethics

Non-partisanship and impartiality are at the heart of these codes. The values of respect for democracy, respect for people, integrity, stewardship and excellence are the foundation for all work of federal public sector employees, including official use of social media.

The following examples demonstrate the values and behaviours that public servants are expected to integrate into decisions and actions when using social media for official purposes.

Respect for Democracy

Uphold the system of Jamaican parliamentary democracy and its institutions by using official social media accounts in a non-partisan and impartial manner at all times.

Respect for People

Treat all people with respect, dignity and fairness and ensure that the use of official social media accounts is respectful of all individuals and groups at all times.

Integrity

Uphold the highest ethical standards and enhance public confidence in the honesty, fairness and impartiality of the public sector by using official social media accounts with integrity and in a manner that bears the closest public scrutiny. Ensure that official social media accounts are never used to inappropriately obtain a personal advantage or to advantage or disadvantage others. Use official social media accounts in such a way as to maintain the employer's trust at all times.

Stewardship

Use and care for public resources responsibly by ensuring that the public money, property and resources dedicated to the official use of social media are used effectively and efficiently.

Excellence

Demonstrate professional excellence in the design and delivery of programs and services through official social media. Provide these programs and services in a fair, timely, efficient and effective manner that respects Jamaica's official language. Work to continually improve the quality of programs and services supported through official social media and promote engagement, collaboration, teamwork, learning and innovation.

Appendix B: Sample Template – Ministerial Social Media Strategy

A social media strategy guides the social media activities of a Ministry. It is a strategic document that explains how the official use of social media supports the ministerial mandate and program objectives. It also provides the Ministry with a clear rationale and intended outcomes for using social media platforms. The following sample template includes the social media strategy elements suggested in this guideline. It is provided here for your consideration.

Overview

This section presents an overview of the ministry's social media presence to date and the context in which it has taken place. This may include background information on previous social media efforts and contextual information from both an overall Government of Jamaica perspective and from the perspective of the ministry.

Business Value and Objectives

This section outlines the business value and objectives of engaging with Jamaicans on social media platforms and how these objectives relate to the ministerial mandate. A clear articulation of this element will enable measurement of the strategy's success, once it is implemented.

Governance and Resources

This section describes the governance and resources allocated to official social media activities. It also identifies the ministerial coordinator for official social media accounts.

Strategic Approach

This section explains the strategic approach to using social media platforms in line with the ministry's objectives and target audiences.

Defining and Measuring Success

This section presents the tools and criteria that will define and measure the success of the social media strategy and the effectiveness of its approach to meeting its objectives.

Integrating Lessons Learned

This section explains the strategic approach to integrating lessons learned and supporting continuous improvement.

Appendix C: Sample Template – Social Media Implementation Plan

An implementation plan is a tool that is aligned with the ministerial social media strategy. Its aim is to help ensure that the key factors for properly establishing and managing official social media accounts are considered during the implementation process. Ministerial heads of communications approve official social media accounts, including those that already exist, based on their corresponding implementation plans.

It is important to plan in detail how an official social media account will be used and implemented. Without proper planning, it may be difficult to meet basic expectations regarding content development, engagement and overall management of the account. There may also be increased risk of non-compliance with legal or policy obligations.

The following sample template is provided to help guide the development of an implementation plan for a proposed official social media account.

Social Media Platform:
Name of account:
Name of account in other language (if applicable):
Implementation plan prepared by:

a) Objectives and Business Drivers

This element outlines how the account aligns with the ministerial social media strategy and articulates the rationale and objectives it aims to achieve.

- How is this account linked to the ministerial mandate and social media strategy?
- What are its key business drivers and objectives?
- What are the proposed uses of this account?

b) Choice of Platform

This element describes the target audience and key considerations that determine the appropriate platform selection and use.

- Who is the target audience?
- What key considerations were used to select this platform? For example:
- What accessibility options are available for the platform, and by what alternative means can the platform be accessed?
- What terms of use apply, and is there any policy or legal compliance issue?

c) Allocation of Resources

This element identifies the human and financial resources that will be dedicated to managing the account.

1. What staff will be working on this social media initiative, and during what intervals?
2. What financial resources will be dedicated to this social media initiative (including resources for training staff)?

d) Roles and Responsibilities

This element identifies the roles and responsibilities of those who will be involved in using and managing the account. In this section, identify the ministerial areas that will be responsible for each key function.

Role and/or Function (add others as needed)	Area of Responsibility
Drafting content	
Approving content	
Publishing content	
Managing the account (administering, monitoring, responding)	
Issues management (responding to issues related to the account should they arise)	

e) Risk Management Plan

This element involves identifying and assessing the risks associated with participating on the social media platform, based on the proposed use, and developing appropriate mitigation strategies.

- Describe the risks and mitigation strategies identified through the risk management exercise (departments may be able to leverage the Government of Jamaica's pre-review of platforms, as described below).

f) Government of Jamaica Privacy Impact Assessment and Threat and Risk Assessment

If the selected platform is on the list of pre-reviewed platforms and the proposed uses for the account are similar to uses identified in the Government of Jamaica Privacy Impact Assessment (PIA) and Threat and Risk Assessment (TRA) for social media, then the ministry can leverage the Government of

Jamaica PIA and TRA. Note that the PIA, including the Government of Jamaica PIA, needs to be signed by the ministerial access to information and privacy coordinator.

If the selected platform is not on the list of pre-reviewed platforms, or the planned uses differ from the uses identified in the Government of Jamaica PIA and TRA, the department needs to conduct its own assessment of risks and share the results of these assessments with the entity.

- Indicate if the Government of Jamaica PIA and TRA apply to this account.

g) Management Protocols

This element describes the management processes that ensure effective, open and transparent engagement practices.

- Describe the protocols that will apply to this initiative:

    - Interaction and content protocol (engagement protocols)
    - Moderation protocol, including a protocol to deal with contentious issues
    - Content style guide (voice and tone of the account, types of content to be posted)
    - User management (who has access to the account, in what capacity, for how long)
    - Business continuity plan

h) Performance Measurement

This element describes the approach that will be used to measure success in meeting the objectives of the account. See Appendix D of this guideline for examples of performance measures and tactics.

- How will success be defined?
- What metrics will be used to measure success?

i) Communications Plan

This element helps align key messages communicated through the official social media account with messages delivered through other ministerial channels.

- What is the communications plan for this initiative?

j) Phasing Out

This element describes the exit strategy to determine when and how to shut down an official social media account (i.e., the conditions that would prescribe an official social media account to be closed).

Short-term accounts are discouraged. In most cases, a combination of the proper use of tags, links and targeted messaging is likely to serve the purposes of a short-term account.

- How, when and why will this account will be phased out?

Appendix D: Sample Template – Performance Measurement

Measuring performance is important to determine whether the use of the official social media account is advancing the ministry's objectives. The table below lists examples of performance measures and tactics for a variety of possible desired outcomes. It is recommended that ministries choose measures that are accurate and feasible to collect.

Desired Outcomes (examples)	**Tactics (examples)**	**Measures (examples)**
Users are aware of new information posted to the website	Leverage existing content by posting it on social media channels (for example, tweet links to recently updated web content)	• Number of real and influential followers • Volume of re-tweets, replies and/or direct messages from followers • Click-throughs to website • Per-cent increase in mentions of issue, theme, department, program or campaign hashtag • Volume of positive and negative mentions
Increased use of web resources	Tweet links to website updates, features and services	• Per-cent increase in followers for specified time period • Per-cent click-throughs to content that leads to the desired action (for example, applying for a grant or program) • Per-cent increase in web traffic from social media • Per-cent shares and referrals of web content and materials

Desired Outcomes (examples)	Tactics (examples)	Measures (examples)
Increased use of ministerial video productions	Publish existing video content (i.e., archives)	• Number of video views to evaluate cost-efficiency • Number of shares of web content • Number of video embeds • Number of referrals from video pages
Increased collaboration with other ministries	Feature related information or services provided online by other local or international jurisdictions	• Number of click-throughs to external content • Volume of re-tweets, replies or direct messages from followers • Number of shares of external content • Number of video embeds • Number of referrals from video pages
Increased awareness of issue or theme	Develop effective playlists to help viewers navigate content	• Number of video views in playlists • Number of referrals to playlists from external sources (other than YouTube) • Number of shares of web content • Number of video embeds • Number of referrals from social media • Per-cent change in web visits resulting from theme-related searches • Per-cent change of onsite searches for issue or theme • Click-throughs to website (for example, by specific theme or issue) • Per-cent increase in mentions of issue, theme, department,

Desired Outcomes (examples)	Tactics (examples)	Measures (examples)
		program or campaign hashtag
Increased interaction with online audiences	Enable a comments feature and moderate accordingly	• Ratio of ministerial posts to interactions from others • Tone and quality of comments and replies • Volume of conversations with public via social channels

This Page Intentionally Left Blank

Guidelines for Cloud Computing

1. Synopsis

The GoJ recognises that citizens and the private sector expect government services to be responsive to their needs and available where and when they want them. Key to realising this vision is the effective use of ICT by government, including the adoption of cloud services. To do this, government agencies need to think and act smarter when it comes to investing in ICT. The availability of cloud services offers an opportunity for government to deliver services more efficiently, as well as providing services that are more responsive to business and community needs. These guidelines aim to drive a greater take up of cloud services by government by adopting a 'cloud too' approach. Both the options of on-site computing and Cloud computing services should be considered and are encouraged to adopt cloud where it is fit for purpose, provides adequate protection of data and delivers value for money.

2. Background

Government ICT investment is increasingly influenced by fiscal constraints, rapidly changing technology and a higher standard of service delivery demanded by citizens and businesses. Cloud services have the potential to address these issues by improving the scalability, responsiveness and reliability of ICT services and providing the agility to meet changing government needs. This approach to ICT sourcing and management may be critical to achieve value, drive innovation and support sustainable investment.

The American National Institute of Standards and Technology (NIST) defines Cloud Computing as: "*a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*"

Three common service models for Cloud offerings include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). For additional details on these, kindly search for NIST Definition of Cloud Computing.

The use of Cloud Computing Services must adequately address relevant acts and Guidelines requirements associated with its ICT systems, including issues of ICT security and risk management, privacy, legal issues (e.g., Terms of Service), records management, and other applicable requirements.

Since Cloud Computing can offer benefits in the cost, performance, and delivery of ICT services, it is anticipated that the use of Cloud Computing services will grow significantly over the next several years. These guidelines are intended to ensure that the use of these services is managed in accordance with existing legislative requirements, and to provide a level of Chief Information Officer (CIO) oversight to address the possibility of a higher level of risk existing as a result of these new and still-evolving ICT service models. The primary reason for this Manual is to facilitate a well-managed and successful adoption of Cloud Computing by establishing a process that directs attention to ICT-related requirements, management processes, and risk factors.

3. Scope

This Manual applies to any acquisition of Cloud Computing services. Project Managers must coordinate planning with operating unit IS Directors / CIOs early in the planning process to avoid unnecessary problems later in the planning and acquisition lifecycle.

This Manual pertains to the acquisition of services from a source outside of the . Internal Cloud Computing services are already covered by existing requirements.

4. The Guidelines Statement

Effective immediately, the Office of the CIO of Jamaica requires that ***evaluate*** *Cloud Computing Services as an alternative for new ICT investments unless otherwise advised for specific reasons of national security. The requirement to consider Cloud Computing Services covers all projects, which have been defined elsewhere as Core, Common or MDA Specific / Local. These projects cover the entire spectrum of ICT services including development, modernization, updates and enhancement as well as steady state operations.*

The has identified the adoption of cloud-based ICT services as a key option in driving better value ICT investment and improving the agility, scalability and reliability of ICT services.

All of the will evaluate cloud-based services when undertaking ICT procurements to determine the ICT delivery model that provides the best value sustainable investment, taking account of the full range of cost-benefit considerations.

As a fundamental part of any business case, careful evaluation of an ICT delivery model is required for any solution, whether delivered through traditional in-house methods or cloud services. While not all government information or ICT will be suitable for cloud, where appropriate cloud services could support ' strategic transition to a service orientation.

5. Benefits of Cloud Services

Cloud-based ICT services provide opportunities for organisations to achieve better value, flexibility and reliability, and make sustainable service delivery improvements:

• *Cost* – Moving from customising and operating in-house ICT to using the best available 'off the shelf' commodity solutions could reduce the total cost of ownership. Flexible, on-demand services enable solution testing without significant capital investment and provide transparency of usage charges to drive behavioural changes within.

• *Consumption based pricing* – The benefits of consumption based, pay-as-you-go pricing enables movement to a model that is aligned to actual demand.

• *Agility* – On-demand, scalable and flexible services that can be implemented quickly provide the ability to respond to changing requirements and peak periods.

• *Innovation* – Innovation will be facilitated by rapid and continuous system development.

• *Resilience* – A large, highly resilient environment reduces the potential for system failure. The failure of one component of a cloud-based system will have less impact on overall service availability and reduce the risk of downtime.

6. Guidelines

GoJ use of Cloud Computing Services must be formally authorized in accordance with the approved **ICT Governance Framework** and specifically must respond to the following **six guidelines**:

- *Use of Cloud Computing Services must comply with all current laws, ICT security, and risk management policies.*
- *Use of Cloud Computing Services must comply with the Access to Information Act and privacy regulations, and appropriate language must be included in the vehicle defining the Cloud Computing source responsibilities for maintaining privacy requirements.*
- *For external (over-seas) Cloud Computing services that require users to agree to terms of service agreements, such agreements must be approved by the Office of the Attorney General of Jamaica or as delegated to individual .*
- *All use of Cloud Computing Services must be approved in writing by the Head of the MDA unit. The senior ICT staff in that MDA unit should certify that security, privacy, and other ICT management requirements have been adequately addressed prior to approving use of Cloud Computing Services.*
- *Project Managers must retain the above certification along with other investment documentation.*

7. Further Guidance

Many issues should be considered carefully before adopting a Cloud Computing solution. Government-wide authorizations of Cloud computing services may be leveraged to facilitate use of these services through the Office of the CIO. However, CIO authorization alone is not sufficient to preclude other requirements for use of a particular service for a particular purpose. Each MDA must designate an Authorized Official, sufficiently familiar with the context of this Manual and Policies and Standards and adequately informed of the associated risks through a Risk Assessment, must document an acceptance of risk and formal authorization of the use of the service.

The list below features some of the more important issues to consider, and to address in contract language when appropriate:

a) Determine why the agency needs to use a Cloud Computing approach. What are the drivers? Several possible drivers are listed below.

- More efficiency or effectiveness for the ICT investment.
- Need for a specific Cloud Computing characteristic (elasticity, scalability, usage-based model)
- Need for rapid implementation (e.g., use of an existing infrastructure, or leveraging of Government-wide authorization)

b) Be realistic in cost estimates. Consider the total lifecycle costs, not just the cost of implementation.

c) Assess Acquisition strategy

- Identify and consider appropriate existing contracts and Cloud Computing solutions already in use at other before acquiring new services.
- When acquiring new services, consider how services can be architected and agreements written in a way that would enable broader use/adoption of the service across the rest of the . **Pay specific attention to consequences of delayed payment or non-payment for cloud services and your ability to continue to access the cloud.**

d) ICT security

- Match ICT security requirements and the security capabilities of the Cloud Computing implementation to those of the mission/business needs being supported.
- Weigh the security threats and opportunities that are present for public, private, and community clouds

- Consider how issues of logging, incident reporting, response, forensics, and other security-related functions should be addressed with respect to the Cloud Computing service provider.
- Consider how disaster recovery and continuity of operations planning will be addressed.

e) Privacy impact

- If Personally Identifiable Information (PII) or other sensitive information is involved, document how it will be protected and who is allowed access to it.
- If the Cloud Computing source is keeping user usage statistics, consider the privacy implications involved and define appropriate safeguards to assure user privacy is maintained. This would include session logs and security access logs, among others.
- Define how all relevant Privacy considerations will be dealt with and identify responsible parties.

f) Pay Attention to Records and Information Management (RIM)

- Identify all systems of records to be hosted in the cloud.
- Identify the schedules for all records and include the information on retention as part of the agreement with the vendor.
- Specify the retention time for all system backups.
- Consider how records management and electronic discovery will be managed in the cloud environment.

g) Consider implications of using a service model that is different from the traditional use of Government-owned and -operated infrastructure.

h) Consider the existing organisational environment when adopting new delivery models. The transition to an as-a-service model may have significant *change management* implications.

i) Identify which issues should be explicitly documented in service level agreements (SLA) with the cloud provider.

j) Consider issues of interoperability with existing systems.

k) Consider issues of data ownership and portability. How would you migrate from a given cloud computing infrastructure to another one at some point in the future?

l) Examine the need for additional training for MDA and ICT staff.

m) Focus on the requirement driving the need, not the technology used to implement it.

n) Determine how mature the industry offerings are for the implementation under consideration.

o) Consideration of open standards, security, interoperability, and data portability are recommended in order to reduce the risk of technology lock-in and inadequate data portability.

p) Include technical aspects since the use of a cloud service will require consideration of LAN, WAN and bandwidth, security, compatibility with the various browser technologies, and implications for longer term data integration. Pay particular attention to licensing as existing software licensing models may not seamlessly translate to a cloud deployment solution.

q) Consider Business Continuity - As with all ICT delivery options, Business Continuity and Disaster Recovery plans should be well documented.

r) Contractual provisions with cloud providers should:

- explicitly state that the is the owner of all rights, title and interest in the data and that all data will be maintained, backed up and secured until returned on termination of the agreement (unless other provisions are made for the migration, transfer or destruction of the data)
- identify the actual geographic locations where data storage and processing will occur
- confirm the jurisdiction which governs the operation of the contract, and application of privacy, confidentiality, access and information management laws
- confine data storage and processing to specified locations where the regulatory framework and technical infrastructure allow the to maintain adequate control over the data.
- Prohibit any unauthorised access, use or alteration of the data.

s) Treat the move to cloud services like any other ICT project (and not simply an incidental aspect) and prepare both a **Business Case** as well as a **Project Charter** for it detailing all the above considerations.

8. References and Additional Information

A wealth of information exists about Cloud Computing and other topics regarding the implementation of Cloud Computing in government.

The links below are the most current documents from the US Federal CIO Council, General Services Administration, National Institute of Standards and Technology (NIST), and the National Archives and Records Administration (NARA).

The General Services Administration and the Federal CIO Council have prepared a document entitled "Security Controls, Guidelines and Process for US Government Cloud Computing," which should also be referenced.

Privacy Recommendations for the Use of Cloud Computing by Federal departments and Agencies

Overview and Issues for Implementation of the Federal Cloud Computing Initiative

A REPORT ON FEDERAL WEB 2.0 USE AND RECORD VALUE

The Federal Risk and Authorization Management Program (FedRAMP)

NIST Cloud Computing Program

Guidance on Managing Records in Cloud Computing Environments

Government of New South Wales Cloud Services Policy and Guidelines

Government of Australia Cloud Computing Policy and Guidelines

US Federal Cloud Computing Strategy

9. Point Of Contact

For additional questions regarding this Manual, please contact:

The Office of the CIO, Jamaica

Ministry of Science, Energy & Technology

(876) 929-8990

eGovJA Ltd.

235B Old Hope Road,

Kingston 6

(876) 927-1125

1. Approvals

Approval Form / Signatures:

Decision:

- ☐ Approved and execution is authorized
- ☐ Approved, but deferred until further notice
- ☐ To be revised and resubmitted for approval
- ☐ Rejected

(Name)	(Name)
(Title)	(Title)
(Date)	(Date)

The signatures of the persons above relay an understanding of the purpose and content of this document by those signing it. By signing this document you agree to this as the formal **GOJ ICT Policies, Standards & Guidelines Manual**.