NDMA NATIONAL DATA
MANAGEMENT AUTHORITY

Secure Use of
Social Media Guidelines

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	Muriana McPherson	31-03-2023
General Manager (NDMA)	Christopher Deen	31-03-2023

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	1.0		General Manager, NDMA	National ICT Advisor

Summary

1. This guideline provides measures for the secure use of social media.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

The purpose for these guidelines is to provide best practices for the secure use of social media to enable collaboration and transparency within the Public Sector organisations of Guyana.

Social media referred to in these guidelines are web-based publishing and communications technologies, such as blogging, social networking, forums, wikis, and file sharing. They are called "social" because they are designed for creating dynamic human networks and exchanging user-generated text and rich media, such as audio and video. They are among the most widely used technologies on the Internet.

Social media encourages collaboration and communication; however, it carries significant dangers ranging from accidental misuse to intentional criminal abuse. Risks to information and computer systems are significant. The use of social media is ever-changing and therefore the dangers and risks also vary. Information and systems security professionals must be both vigilant and creative in responding to the shifting risk environment.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this guideline. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This guideline encompasses all users of information systems, and systems that are automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user's responsibility to read and understand this guideline and to conduct their activities in accordance with its terms.

4.0 Guidelines

4.1 Security Risks

Cyber criminals target social media sites because they offer an effective means of propagating malicious code to a wide, unsuspecting audience. Sites that allow user-generated content are among the most active distributors of malicious content, such as worms that can shut down networks, or spyware and keystroke loggers that can compromise organisation data. Many postings to blogs, chat rooms and message boards may be spam or contain malicious links. Since many links on social media sites are in the form of shortened or condensed URLs, a user is unable to determine where these links lead, making it easy for criminals to direct an unsuspecting user to malicious sites. The false sense of a trusted community when visiting social media sites increases the likelihood that a user may fall victim to this type of threat. If an employee is using the organisation's resources when this occurs (e.g., a work PC), these resources have an increased risk of becoming infected.

Many social media sites do not have adequate security controls to protect the information they are holding. For example, some sites do not require strong passwords, some transmit credentials in clear text and some use easily guessed "secret" or "challenge" questions. As a result, social media accounts are frequently compromised. If the same account credentials are used for both the external social media site and organisation's resources, this could lead to unauthorised access to the resources of the organisation.

Allowing access to externally hosted social media sites, an agency may inadvertently bypass its own security controls. For example, external instant messaging and email services, which may be blocked within an agency because of security concerns, may be accessible through applications available on externally hosted social media sites.

Inadvertent exposure of confidential information is another risk associated with the use of social media. The ease of posting all types of content (e.g., documents, photos, videos, audio recordings) to social media sites, coupled with the erroneous assumption of a trusted environment, may result in the disclosure of confidential information.

Use of social media sites leads to a greater web presence, which in turn leads to a greater risk of spam and targeted phishing attacks. Some social media sites harvest information from email contact lists, which may put agency contact information in the hands of a third party with no knowledge of how that third party will use and/or protect that information. Information about a user's professional role in government, including organisation email addresses, should not be included on personal profiles. With the wealth of information available on social media sites, hackers are using tools to correlate information into a detailed user profile which can then be used for targeted phishing and other social engineering attacks.

Once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups and memory cache. Some social media sites may claim to own the content posted on their site.

4.2 Mitigation of Risks

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of social media:

4.2.1 Governance and Use

4.2.1.1 Use of social media on behalf of an organisation or access to social media from organisation resources should be at the discretion of executive management.

4.2.1.2 Authorise use of social media after a proper evaluation of risk and demonstration of a justified business need.

4.2.1.3 Develop acceptable use policies to include social media and publicise these policies to users.

4.2.1.4 Educate users on *acceptable use policy* and the risks associated with social media as part of the organisation’s annual security awareness training.

4.2.1.5 Do not use the same passwords for social media sites as are used to access organisation’s resources. Likewise, do not use the same password on more than one social media site.

4.2.1.6 Classify data prior to posting per the Information Classification Standard.

4.2.1.7 Do not post any non-public records (e.g., documents, photos, videos, audio recordings) without following an established process, consistent with policy on information security that includes documented approval from agency management.

4.2.1.8 Do not post any personally identifying information (PII) on social media sites.

4.2.1.9 Where possible, minimise the posting of information about one’s role in an organisation, including organisational email addresses, on social media sites.

4.2.2 Technological Controls

4.2.2.1 URL and IP Filtering: This technology blocks certain websites, parts of websites, or IP addresses. This can help protect users who may be redirected to a known malicious site. In addition, for some social networking sites, using URL filters to block the login pages for all but those employees with a business need, allows for access to public information while preventing access to applications and messaging tools that may bypass security controls.

4.2.2.2 Malware Filtering at the Network Perimeter: This technology inspects traffic before it gets into an organisation’s network to ensure that it does not contain malware and blocks any malware that it finds.

4.2.2.3 Intrusion Detection/Intrusion Prevention Systems**:** This technology provides near real time monitoring and analysis of network activity for potential attacks in progress.

4.2.2.4 Data Loss Prevention: This technology is designed to detect and prevent the unauthorised use and transmission of confidential information. It should be used at both the desktop and the web gateway to monitor for and block outbound confidential data.

4.2.2.5 Browser with Restricted Privileges: If available, this feature ensures that the browser and its add-ons run with a minimal set of permissions preventing the installation of malicious code.

4.2.2.6 Web Reputation Services: These services test websites for spam, spyware, scams etc. and use those tests to give safety ratings to help users avoid visiting unsafe sites.

4.2.2.7 Moderating Content: When hosting an organisational social media site, establish a process which would allow the host to moderate (i.e., preview, accept, reject) content submitted to the site prior to its being posted (i.e., made visible to visitors). This helps the host to block content containing malicious links or inappropriate content.

4.2.2.8 URL Shortening Preview Tools: These tools display the actual URL destination masked by shortened URLS from services such as TinyURL and Bit.ly. The preview allows users to make informed decisions about links before clicking.

4.2.3 Policy Controls

4.2.3.1 Organisations must follow all provisions of the *Information Security Policy* to facilitate the protection of information assets, including hosted social media sites available to the public (e.g., wikis, blogs), whether on organisation's infrastructure or hosted at an outsourced provider under contract. This includes, but is not limited to:

4.2.3.1.1 Public Website Content Approval Process**:** A process must be established for reviewing and approving updates to publicly available content. These reviews must consider the type of information being made available, the accuracy of the information and potential legal implications of providing the information, such as confidentiality and copyright issues.

4.2.3.1.2 Vulnerability Scanning**:** All hosts that are or will be accessible from outside the organisation's network must be scanned for vulnerabilities and weaknesses.

4.2.3.2 To further protect hosted sites, as well as to protect resources used to access externally hosted social media (e.g., Facebook, YouTube, Twitter), the following controls from the *Information Security Policy* must also be in place:

4.2.3.2.1 Protection Against Malicious Code: Software and associated controls must be implemented across systems to prevent and detect the introduction of malicious code.

4.2.3.2.2 Software Maintenance: All known security patches must be reviewed, evaluated and appropriately applied in a timely manner to reduce the risk of security incidents.

4.2.3.2.3 Privileged Accounts Management: The issuance and use of privileged accounts must be restricted and controlled. Inappropriate use of these account privileges is a major contributing factor to system breaches. Processes must be developed and implemented to ensure that use of privileged accounts is monitored, and any suspected misuse of these accounts is promptly investigated. Passwords of privileged accounts must be changed more often than normal user accounts.

4.2.3.2.4 Security Incident Reporting: All staff and contractors are required to report any observed or suspected incidents to the appropriate manager and the Information Security Officer/designated security representative as quickly as possible.

5.0 Compliance

These guidelines shall take effect upon publication. Compliance is expected with all organisational guidelines, policies, and standards. Failure to comply with these guidelines may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this guideline shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this guideline.

8.0 Definitions of Key Terms

Term	**Definition**
Malware[1] Malicious code	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
Network[2]	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
PII[3]	Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
SPAM[4]	Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages
Spyware[5]	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

[1] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/malware

[2] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/network

[3] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center (CSRC) - https://csrc.nist.gov/glossary/term/pii

[4] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/spam

[5] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/spyware

Term	Definition
URL Uniform Resource Locator[6]	Reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A typical URL could have the form http://www.example.com/index.html, which indicates a protocol (http), a host name (www.example.com), and a file name (index.html). Also sometimes referred to as a web address.
User[7]	Individual or (system) process authorized to access an information system.
Vulnerability[8]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, National Data Management Authority.

[6] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/uniform_resource_locator

[7] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user

[8] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/vulnerability