Mobile Device Security Standard

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 standard establishes protection standards for the use of mobile devices.
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

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices that are only used within an organisation's facilities and on the organisation's networks. This standard outlines the additional protections required for the use of mobile devices.

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 standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard applies to users of all mobile devices, whether owned by the Government of Guyana or by employees, that access the Government's information systems or infrastructure 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 standard and to conduct their activities in accordance with its terms.

4.0 Standard

4.1 Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and is portable (i.e., non-stationary). These devices come in forms such as: smartphones, PDAs, smart watches, tablets, laptops, and wearable devices. Mobile devices must follow all requirements of the Information Security Policy.

4.2 As per the Encryption Standard, all mobile devices that access or contain any organisation information must be encrypted.

4.3 For organisation issued mobile devices or personal mobile devices with direct access to managed networks, only those applications which are approved may be installed and or run on the mobile devices. Applications must be restricted through the use of whitelisting (preferably) or blacklisting. Applications must be digitally signed to ensure that only applications from trusted organisations are installed on the device and that code has not been modified.

4.4 Organisation information must be removed or rendered inaccessible from mobile devices after no more than 10 incorrect authentication attempts.

4.5 Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes.

4.6 Mobile devices which directly connect to managed private networks, virtually connect to managed private networks in a manner consistent with a directly connected device, or which contain or could contain information, including e-mail data, must be managed by a Mobile Device Management (MDM) or other centralised management solution, and must adhere to the organisation's Remote Access Policy.

4.7 Use of synchronisation services, such as backups, for mobile devices (e.g., local device synchronisation, remote synchronisation services, and websites) must be controlled through an MDM or other centralised management solution.

4.8 Mobile devices may not access private networks unless their operating environment integrity is verified (including whether the device has been rooted/jailbroken).

4.9 Organisations must manage all mobile devices by:

4.9.1 Implementing device policies and configurations as appropriate to the use of the device.

4.9.2 Developing and implementing processes which check for upgrades and patches to the software components, and for appropriately acquiring, testing, and deploying the updates to organisation issued devices.

4.9.3 Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.

4.9.4 Detecting and documenting anomalies which may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.

4.9.5 Providing training and awareness activities for mobile device users on threats and recommended security practices which can be incorporated into the organisation's security and awareness training.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with this standard 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 standard 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 standard.

8.0 Definitions of Key Terms

Term	Definition
Mobile Device[1]	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. See portable storage device.
Mobile Device Management[2]	The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices.
User[3]	Individual or (system) process authorized to access an information system.
Whitelisting[4]	1.An approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition. 2.An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments.
Blacklisting[5]	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.

[1] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/mobile_device
[2] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/mobile_device_management
[3] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/user
[4] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/whitelisting
[5] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/blacklisting

Term	Definition
Synchronisation[6]	The process of setting two or more clocks to the same time.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

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