	Document Title	Document Number	Issue Date
سدرة للطب Sidra Medicine	**MOBILE COMPUTING SECURITY**	**540**	**16/12/2019**
	Approved By	**Version Number**	**Review Due Date**
POLICY	**Nasser Alawad – Acting Chief Information Officer**	**2**	**16/12/2021**

If you print this document from the Electronic Manual, the copy is valid only until midnight of the day you printed it.

SCOPE	Organizational ☐ Departmental ☒
TITLE	Mobile Computing Security
PURPOSE	Document the necessary controls to minimize information security risks affecting the organization, from laptops, mobile devices, and mobile storages misuse, compromise, and loss.
APPLICABLE TO	Mobile computing and storage devices that will be securely managed by the authorized Sidra staff, vendors and third party contractors.
DEFINITIONS	
EXPECTED OUTCOME	Controls and security best practices to be implemented and applied to ensure a secured and controlled use of the organization's mobile devices.

POLICY STATEMENT

1. GENERAL STATEMENTS

1.1 The use of all Mobile Computing Devices such as laptop, portable digital assistants (PDAs), smart phones or other portable storage devices not classified as a desktop workstation shall be justified by a business need and approved by the respective lines of management.

1.2 Users of laptop computers or other electronic data mobile devices shall exercise reasonable care to protect the organization's data.

1.3 A list of organization-owned Mobile Computing Devices shall be maintained and verified periodically.

1.4 Wherever feasible, laptops should be physically locked when left unattended (using wire locks).

1.5 In the event an organization-owned Mobile Computing Device is lost or stolen, the theft or loss shall be immediately reported to the police authorities and Security Operations.

1.6 Emergency destruction/locking plan /remote wipe/auto destruct controls shall be put in place for theft of any Mobile Computing Devices.

2. DATA STORAGE, TRANSMISSION AND ENCRYPTION

2.1 The organization's approved encryption tools shall be enabled on Mobile Computing Devices that transmits or store confidential and highly confidential information such as ePHI, financial data, and strategic information.

2.2 Procurement of Mobile Storage Devices shall be authorized by the Enterprise Cyber Security and Governance Department.

3. DEVICES SECURITY

3.1 Sidra holds the right to install a security application on any device which has access to the corporate network or holds sensitive data. In the event of termination of employment, Sidra reserves the right to remove content from the device.

3.2 All Mobile Computing Devices shall be configured as per the Antivirus Policy to adequately protect them from malwares, spywares and adwares.

3.3 Device passwords are required on all Sidra owned mobile devices that have corporate directory or company email access.

3.4 Following the termination of an end user's contract, Sidra owned Mobile Computing Device shall be immediately returned.

3.5 The mobile device shall be wiped clean of all organization data, including but not limited to: corporate directory, emails, applications and stored data.

COMPLIANCE REFERENCES	1. International Organization for Standardization (ISO) 27001:2013 1.1 Mobile device policy (A.6.2.1) 1.2 Security of equipment and assets off-premises (A. 11.2.6) 2. Ministry of Transport and Communication (MoTC) - National Information Assurance Policy v2.0. 2.1 Portable Devices and Working Off-Site Security [OS] – (Section 11.2) 3. MoPH- RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	
REFERENCES	
NAME OF AUTHOR	Naoufal Rihani, Head of Information Security
POLICY OWNER/ DEPARTMENT	Mostafa Essemmar, Director – Enterprise Cyber Security and Governance
APPROVAL BODY	As per Executive Committee Delegation of Authority for Policy Approval (V.4 12 August 2018)
MEASUREMENT OF COMPLIANCE	Periodic Security Audits Annual Effectiveness Review
KEYWORD SELECTION	Keyword 1 : Mobile Device Keyword 2 : Laptop Keyword 3 : Mobile Storage Keyword 4 : Encryption

Version Number	Issue Date	Summary of amendments Key Changes	Communication Message
1	21/04/2016	New policy	
2	16/12/2019	1. Deleted the definitions of Mobile Computing Device, Mobile Storage Device and Encryption as they are straight forward to understand by the reader. Incorporated them in the policy statements 1.1 and 2.1 for more clarity. 2. Moved ISO 27001:2013 and NIA from References section to Compliance References. 3. Modified statement 1.4 related to mandating the use of laptop wire locks 4. Removed the statement 1.5 related to Mobile devices with recording facilities 5. Removed statement number 2.1 related to prohibition and of use of Mobile Storage devices and Security approval requirement. 6. Added statement 2.2 related to procurement of Mobile Storage devices 7. Removed statement 3.3 related to SIM card lock control	Departmental Policy will be published in the portal and will be communicated to respective staff through departmental means.