سدرة للطب Sidra Medicine	Document Title	Document Number	Issue Date
	Mobile Computing Security		**21/04/2016**
		Version Number	**Revision Date**
POLICY	APPROVED	**#1**	**30/06/2018**

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

DEPARTMENT	Organizational ☐ Departmental ☒ Name: Information Management
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 IT staff, vendor and third party contractors.
DEFINITIONS	**Mobile Computing Device -** laptop, portable digital assistants (PDAs), smart phones or other portable storage devices not classified as a desktop workstation. **Mobile Storage Device -** hardware device used to record and store data such as USB, iPod, CD, DVD and Fire wire Hard Drives **Encryption -** conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
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 Mobile Computing Devices 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 Laptops shall be physically locked (using wire locks) when left unattended in public areas, either inside or outside the organization. 1.5 Mobile devices with recording facilities are not allowed into high risk areas (e.g. data centers). 1.6 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 to IT Security. 1.7 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 use of Mobile Storage Devices is prohibited unless justified by a strong business need and approved by IT Security. 2.2 The organization's approved Encryption option shall be enabled on Mobile Computing Devices that transmit or store confidential and highly confidential information such as ePHI, financial data, and strategic information. **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, the Sidra reserves the right to remove content from the device. 3.2 Mobile Computing Devices shall be adequately protected from malwares, spywares and adware. All Mobile Computing Devices shall be configured as per the Antivirus Policy. 3.3 SIM card lock codes are required on all company mobile devices 3.4 Device passwords are required on all company mobile devices that have corporate directory or company email access. 3.5 Following the termination of an end user's contract, Sidra owned Mobile Computing Device shall be immediately returned. 3.6 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. ISO 27001:2013 Standard** 1.1 Mobile device policy (A.6.2.1) 1.2 Security of equipment and assets off-premises (A. 11.2.6) **2. NIA Policy v2.0** 2.1 Portable Devices & Working Off-Site Security [OS] – (Section 11.2) **3. JCI-** MOI.2 4. **MoPH-** RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	
REFERENCES	1. International Organization for Standardization (ISO). BS ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems – Requirements. ISO/IEC resources; 2013. 2. Ministry of Information & Communication Technology. National Information Assurance Policy v2.0. ICT Qatar resources; 2014. 3. Joint Commission International, Joint Commission International Accreditation Standards for Hospitals. 6th Edition, Joint Commission International: Oak Brook, ILL. 2017
NAME OF AUTHOR	Mostafa Essemmar, Manager- IT Security, Infrastructure & Operations Dept
POLICY OWNER/ DEPARTMENT	Chief Information Officer / Information Technology Services
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