	Document Title	Document Number	Issue Date
السحارة Sidra مركز السحارة للطب والبحوث Sidra Medical and Research Center	INFORMATION ASSETS ACCEPTABLE USE		21 May 2015
		Version Number	First Revision Date
POLICY	APPROVED	#1	20 May 2017
		Version Number	Second Revision Date
		#2	20 May 2019

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 ☐
TITLE	INFORMATION ASSETS ACCEPTABLE USE
PURPOSE	To ensure the appropriate use of organizational assets to prevent exposing the organization's network to risks including exposure of critical information, integrity of data and other legal issues. These rules are in place to protect the employees, contractors and the organization.
APPLICABLE TO	All staff authorized to access the organization's information or who have been granted access to systems or applications. All business partners; business associates; full-time, part-time, and temporary employees; contractors; consultants; and vendors.
DEFINITIONS	▪ **Asset** - any tangible and intangible resource that has a value for the organization. ▪ **PHI** - Personal Health Information or Private Health Information ▪ **ePHI** - Electronic Personal Heath Information
EXPECTED OUTCOME	Organization's assets use by employees and contractors to be regulated and controlled by the rules set out in the policy statement.
POLICY STATEMENT	**1.0 GENERAL USE AND OWNERSHIP** 1.1 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Reasonableness of personal use is defined as "no impact on employees' productivity, organization's security and service delivery". 1.2 Access to organization's IT Resources shall be used only for the purpose for which the employee/contractor is authorized. 1.3 Use of organization's IT Resources is not considered private, and users do not have the same personal privacy rights when using these devices as they would when using private communication devices. **2.0 PERSONAL HEALTH INFORMATION** 2.1 The employees/contractors processing, accessing, storing, or communicating PHI or ePHI are responsible for any disclosure or loss of data resulting from their activities. 2.2 Employees/contractors must ensure through legal or technical means that PHI and ePHI remains within the control of the organization at all times. 2.3 Conducting activities that results in the storage of ePHI on personal or non-organization controlled environments, including devices maintained by a third party with whom the

organization does not have a specific contractual agreement, is prohibited.

2.4 Any media containing PHI, e.g. CDs, USB, etc. must be treated with the same security standards that apply to the original file.

3.0 CONFIDENTIALITY AND INFORMATION DISCLOSURE

3.1 All employees and contractors shall sign a "Confidentiality Undertaking" as part of their contract.

3.2 If work is contracted to a 3rd party who in the course of their work may require access to confidential information or PHI, the 3rd party will be required to sign the appropriate Confidentiality Agreement for external contractors.

3.3 The Internet is a public network; therefore employees and contractors must not transmit sensitive or confidential organizational information over the Internet.

3.4 Employees, personnel, or third party contractors shall not publicly disclose internal information via the Internet that may affect the organization.

3.5 Users must not post network or server configuration information about any information systems to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.

3.6 It is prohibited to run any programs that reveal security weaknesses in any organization's IT system.

3.7 Users must ensure that postings on to mailing lists, public news groups and related websites do not reveal details of the organization internal functioning, infrastructure or potential vulnerabilities. If such data must be transmitted for a legitimate business need, it must be in an encrypted format.

3.8 Employees shall keep in mind that all messages transmitted over the Internet from the organization's computing resources bear the organization's specific Internet Protocol [IP] address and may be attributed to it.

3.9 Individuals are responsible for all electronic messages or files originating from their PCs using their user ID.

3.10 Creating personal web pages which are hosted on the organization resources is prohibited.

3.11 It is prohibited to download large media files, unless with an authorized business case.

3.12 It is prohibited to make unauthorized copies of configuration files.

3.13 Install, connect, or use of non-official unauthorized hardware within the organization's network is prohibited.

3.14 Use of non-organization official email account for work purpose, transmission of data or backup of files is prohibited.

3.15 It is prohibited to install a type of security software (Antivirus, scan tool, etc.) which has not been authorized by the IT Security Department.

3.16 Users shall not install unauthorized third party software or code on any organization's PCs and other systems.

4.0 COPYRIGHT

4.1 Violations of any software which is protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "Pirated/Cracked" or other software products that are not appropriately licensed for use by the end user or the organization is prohibited.

4.2 Unauthorized copying and/or distribution of any copyrighted material including, but not limited to, digital magazines, eBooks, which the organization or the end user does not have an active license is prohibited.

5.0 ACTIVITIES LOGGING AND MONITORING

5.1 Users are to be aware that in accordance with *System Security Monitoring Policy*, all activity on the IT resources is continuously monitored and audited and these records are archived. If necessary these records can be used as evidence in any legal or disciplinary action.

5.2 In the ordinary course of organization's business, email and web browsing are surveyed, archived and logged by system and security administrators to monitor network efficiency, provide virus protection, filter spam mail, enforcement of data security and compliance.

COMPLIANCE REFERENCES	**1. ISO 27001:2013 Standard** 1.1 Acceptable use of assets (A.8.1.3) 1.2 Terms and conditions of employment (A.7.1.2)

	1.3 Confidentiality or nondisclosure agreements (A.13.2.4) **2. NIA Policy v2.0** 2.1 System Usage Security [SU] (Section 7.2) **3. JCI**- MOI.2 **4. MoPH**- RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	POL – D – System Security Monitoring
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.
NAME OF AUTHOR	Mostafa Essemmar, Manager - IT Security, Infrastructure & Operations Dept
POLICY OWNER/ DEPARTMENT	Chief Information Officer / Information Technology Security
MEASUREMENT OF COMPLIANCE	Periodic Security Audits Annual Effectiveness Review
KEYWORD SELECTION	Keyword 1 : acceptable Keyword 2 : use Keyword 3 : assets Keyword 4 : confidentiality