سدرة للطب Sidra Medicine	Document Title	Document Number	Issue Date
	INFORMATION ASSETS ACCEPTABLE USE	**290**	**13/11/2019**
	Approved By	**Version Number**	**Review Due Date**
POLICY	**Mohammed Khalid Al Mana – Chair, Transition Committee**	**3**	**13/11/2021**

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	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	
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. GENERAL USE AND OWNERSHIP

1.1 Employees are responsible for exercising good judgment regarding the reasonableness of personal use of Sidra's information assets and IT resources. 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. PERSONAL HEALTH INFORMATION (PHI)

2.1 Staff must adhere to the following requirements in relation to the management of PHI and are also directed to Sidra's detailed policies governing the privacy and confidentiality of PHI: (1) "Confidentiality of Personal Health Information" and (2) "Use and Disclosure of Personal Health Information".

2.2 The employees/contractors processing, accessing, storing, or communicating PHI (electronically or otherwise) are responsible for any disclosure or loss of data resulting from their activities where staff have not complied with Sidra policy or Qatar law. Staff must contact at privacy@sidra.org for advice and guidance on handling Patient PHI if they have any queries.

2.3 PHI information is supposed to be accessible to the authorized personnel only through approved clinical systems or applications.

2.4 Sidra staff must avoid saving PHI on the local storage of desktops / laptops and any personal use must be approved by the data privacy working group.

2.5 Sidra staff must not store PHI or any sensitive information which may disclose the health record or personal information of the patient in any manner on the organization's shared folders or SharePoint Portal.

2.6 Conducting activities that results in the storage of PHI on personal or non-organization controlled environments, including devices or software maintained by a third party with whom the organization does not have a specific contractual agreement, is prohibited.

2.7 Any media containing PHI, e.g. CDs, USB, etc. must be treated with the same security standards that apply to the original file. Staff should contact the IT Department or Enterprise Cyber Security & Governance for advice and guidance about potential additional precautions such as encryption and password protection for PHI stored or transferred outside of the organization’s native systems.

3. CONFIDENTIALITY AND INFORMATION DISCLOSURE

3.1 All employees and contractors shall sign a “Confidentiality Undertaking” or other acknowledgement as requested by Sidra which may augment the confidentiality obligations already included in their contract of employment or consultancy agreement.

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 in accordance with Sidra policy “Use and Disclosure of Personal Health Information”.

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 organization’s IT system.

3.7 Users must ensure that postings on 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 supported 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. 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. 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. **National Information Assurance (NIA) POLICY v2.0** issued by the Qatar Ministry of Transport and Communications (formerly Ministry of Information and Communications Technology) 2.1 System Usage Security [SU] (Section 7.2) 3. Joint Commission International, Joint Commission International Accreditation Standards for Hospitals. 6th Edition, Joint Commission International: Oak Brook, ILL. 2017. MOI 2 4. Qatar National Healthcare Facilities MoPH- RCFO.9/RCFH.7/ RCP.10 5. Law No. 13 of 2016 on the Protection of Personal Data Privacy
RELATED DOCUMENTS	POL - D - System Security Monitoring POL - O - Confidentiality of Personal Health Information POL - O - Use and Disclosure of Personal Health Information POL - O - Confidentiality of Non-Patient Information
REFERENCES	
NAME OF AUTHOR	Mostafa Essemmar, Director – Enterprise Cyber Security & Governance
POLICY OWNER/ DEPARTMENT	Chief Information Officer / Information Technology Security
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 : acceptable Keyword 2 : use Keyword 3 : assets Keyword 4 : confidentiality

Version Number	Issue Date	Summary of amendments Key Changes	Communication Message
1	21/05/2015	New Policy	
2	20/05/2017	Amended	
2	13/11/2019	1. Section of Personal Health Information amended to direct Staff to Sidra's detailed policies governing the privacy and confidentiality of PHI: (1) "Confidentiality of Personal Health Information" and (2) "Use and Disclosure of Personal Health Information". 2. Policy statements are reviewed and some are rephrased without changing the meaning of the earlier policy statement. 3. Deleted the definitions of Asset, PHI and ePHI, as they can be understood by policy's intended readers. 4. Added policy statements 2.4 /2.5 /2.6 to address the concerns raised about staff storing the patient data on shared folder / on the local hard drive of desktops / laptops. 5. Removed ISO 27001:2013 and NIA from References section to Compliance References.	The purpose of this policy is 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.