	Document Title	Document Number	Issue Date
السدرة Sidra مركز السدرة للطب والبحوث Sidra Medical and Research Center	**INFORMATION ASSET MANAGEMENT**		**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 ASSET MANAGEMENT
PURPOSE	Provide a set of guidelines to identify, classify and protect dependent information assets (both IT and non-IT) to support critical activities.
APPLICABLE TO	All workforce members with access to the organization 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 -** An asset is any tangible or intangible thing or characteristic that has value to an organization. • **Physical Asset -** Physical facilities where critical information assets process, store, route, or transmit sensitive information. Example: Network & Security devices, Desktops & Laptops, Server, Paper documents, Office equipment, Printers, Magnetic media. • **Information Asset –** any information or information processing facility that has value to the organization and includes: ▪ All data, whether in the form of electronic media or physical records that are used by the organization or in support of business and clinical processes. ▪ All data maintained or accessed through systems owned or administered by or on the behalf of the organization. ▪ All personal, private, or financial data about healthcare patients, workforce members, contractors, consultants, vendors, or other 3rd party entities or business associates, which must be protected in accordance with relevant legislative, regulatory, or contractual requirements. ▪ All the information processed, stored, handled, transmitted, or routed by hardware and software resources. ▪ Records in hard (print) or soft (digital) copy. • **Business Information** - hard- or soft-copy electronic files or printed media containing cost data, price data, proposals, proprietary product information, intellectual property, payroll data, personnel information, contracts, agreements, internal legal, human resources, financial, and accounting information, and any other non-public, non-clinical confidential or restricted correspondence. • **Clinical Information** - personally identifiable information, and protected healthcare information, as defined below, that pertain to healthcare patients and their family members. • **Personally Identifiable Information (PII) -** not necessarily healthcare-related, in the organization's system that can be used to identify an individual and includes: name, address, Qatari identification number or other national identifying number or code (e.g., social security

	number for an American patient), telephone number, and email address. • **Protected Healthcare Information (PHI) -** any information which concerns health status, provision of health care, or payment for health care that can be linked to an individual. PHI is generally categorized as follows: o Names; o Geographical subdivisions that includes a street address; city; or zip code. o All elements of dates directly related to the patient, including birth date (or elements of dates that indicate a patient's age); hospital admission date; hospital discharge date; and date of death; o Telephone and fax numbers; o Email addresses; o Qatar Identification (QID) number, motor vehicle operator's license numbers, medical record numbers; or account numbers; o Motor vehicle identification (license plate numbers, serial numbers, etc.); o Biometric identifiers (finger prints, voice prints, etc.); and o Full face photographic images or comparable images. • **Electronic Protected Healthcare Information (ePHI) -** PHI stored, transmitted, or received in electronic form via any type of electronic media, regardless of whether the transmission of ePHI is person-to-person, person-to-system, system-to-system, or system-to-person. • **Asset Owner -** a person or a group of people who have been identified by the management as having responsibility for the maintenance of the confidentiality, availability and integrity of that asset. The asset owner may change during the lifecycle of the asset, and does not normally or necessarily personally own the asset. • **Asset Custodian -** Asset custodian has the responsibility to maintain the asset as delegated by the asset owner.
EXPECTED OUTCOME	• All information or physical assets to be identified, classified and labelled with the required level of protection.
POLICY STATEMENT	**1. ASSET INVENTORY** 1.1. Information assets shall be clearly identified, categorized and classified. 1.2. An Information Asset Register detailing both the tangible (E.g.; Hardware, tools, facility, people) and intangible information assets (E.g.; Documents, diagrams, Forms, patient information, flowcharts, plans) shall be maintained by the respective asset owners. 1.3. The asset inventory shall include: ▪ Name or unique ID for asset or group of assets ▪ Location of information asset ▪ Asset owner & Custodian ▪ Security classification of the information asset ▪ Units (exact quantity or variable – if continuously changes) ▪ Date of security classification ▪ Retention Period / Expiry Date of Assets 1.4. Level of protection shall be proportional to the asset's criticality and sensitivity. **2. ASSET OWNERSHIP** 2.1. Responsibility shall be assigned for each specific information asset, or group of assets, within each business and clinical department. 2.2. **The Asset owner shall:** ▪ Ensure that assets are inventoried ▪ Ensure that assets are appropriately categorized, classified and protected ▪ Define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies ▪ Ensure proper handling throughout the lifecycle of the asset 2.3. The Information Security Officer in coordination with Asset Owners shall assess the classification level, criticality, and nature of the asset, and then establish appropriate security controls proportionate to the asset's criticality ans sensitivity as required by security policies. **3. CRITICALITY OF INFORMATION ASSET**

3.1. All business and clinical information asset shall be categorized (see Table 1). The category assigned shall primarily reflect the impact on the business mission or the maintenance of patient health and safety should the information system be damaged or destroyed, and the intrinsic replacement value of the information asset.

3.2. The sensitivity of the information handled by the system shall also be considered when determining the criticality of an asset.

3.3. The asset owner, in consultation with the Information Security Officer, shall evaluate the criticality of Assets in terms of High (H), Medium (M) and Low (L).

Table 1:Information Criticality Classification Scheme

Information Criticality Classification Scheme	
Criticality Level	**Definition**
Mission Critical (H)	Information assets identified as mission critical shall be protected to the fullest extent practical. Their loss would be catastrophic and would have an immediate impact on business continuity or patient care. Mission critical information assets must be highest priority for recovery and restoration following a disaster.
Mission Essential (M)	Information assets identified as mission essential usually provide direct support to mission critical assets. Their loss could have an impact on mission critical assets and reduce the ability of the organization to conduct normal business operations. Prolonged loss of mission essential information assets will eventually have an impact on overall organization business continuity.
Non-Mission Essential (L)	Systems identified as non-mission essential require levels of security commensurate with the information they process, store, handle, or route. The loss of these systems will not have an adverse effect on the ability of the organization to continue business and clinical operations.

4. INFORMATION ASSETS SENSITIVITY CLASSIFICATION

4.1. All information shall be assigned to one of the classification level (see Table 2) to assist information owners in determining the relative sensitivity of information that shall not be disclosed outside of the organization without proper authority.

4.2. The information sensitivity classification shall be clearly made visible in all type of media produced or transferred.

Table 2. Information Sensitivity Classification Scheme

Information Sensitivity Classification Scheme	
Classification Level	**Description**
Restricted /Highly Confidential [C3]	Confidential information with access limited to a very small set of persons; material whose disclosure would cause severe damage to the affected party (Board/executive/minister level management changes, decisions etc.). Applies to most sensitive and strategic information, the unwanted disclosure of which can bring substantial damage to the strategic goals, major legal consequences, or severe damage to the organization's reputation (PHI, ePHI, strategic plans, internal audit and investigation reports, etc.).
Limited Access /Confidential [C2]	Access for defined users, roles or user groups, according to specific rules; material whose disclosure would cause serious damage to the affected party (e.g. HR data, sensitive constituent data, etc.). Applies to sensitive business information, the unwanted disclosure of which can bring financial and reputational damages (PII, financial data, security policies, network or system configurations, etc.).

Internal [C1]	For internal use; material whose disclosure would cause light to moderate damage to the affected party. Information which if disclosed may have minimal impact on the organization. This information is not generally releasable to the public and requires a minimum level of protection (employee handbooks, internal telephone listings, and security standards and operating procedures, etc.)
Public [C0]	Information which if disclosed would have no impact on the organization as it is specifically intended for public release (general corporate information on public organization's web site, marketing brochures, and media releases, etc.).

5. INFORMATION LABELLING

5.1. All Sidra assets shall be prominently labelled to ensure that they are given the necessary protection in use, storage and transport.

5.2. All information assets shall be rated in accordance with Sidra Information Sensitivity Classification Scheme. All assets rated with a Confidentiality rating of C1, C2 or C3 shall be suitably marked the respective data label of Internal, Confidential, Highly Confidential.

5.3. All Sidra documents shall be considered as "Internal", unless labelled differently or specifically produced for public release.

5.4. A data labelling system shall be established to support the "Need-To-Know" requirement, so that information will be protected from unauthorized disclosure and use.

5.5. Data labelling education and awareness shall be established for staff, employees and contractors.

5.6. Information may cease to be Confidential/Highly Confidential after a certain period of time; appropriate monitoring & security mechanism shall be deployed to avoid the overspending on the security of assets.

COMPLIANCE REFERENCES	**1. ISO 27001:2013 Standard** 1.1 Inventory of Assets (A.8.1.1) 1.2 Ownership of assets (A.8.1.2) 1.3 Classification of information (A.8.2.1) 1.4 Labelling of information (A.8.2.2) **2. NIA Policy V2.0** 2.1 Appendix B – Asset Classification Model [IAP-NAT-INFA] 2.2 Data Labelling [DL] - Section 4.2 **3. JCI- MOI.2** **4. MoPH- RCFO.9/RCFH.7/ RCP.10**
RELATED DOCUMENTS	POL - O – Information Risk Management PRO - O – Asset Management Procedure
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/	Chief Information Officer / Information Technology

DEPARTMENT	
MEASUREMENT OF COMPLIANCE	Periodic security audits
KEYWORD SELECTION	Keyword 1 : Asset Keyword 2 : Inventory Keyword 3 : Classification Keyword 4 : Labeling