MS-IS-SG-003

Information Security Policies

In Compliance with:

ISO 27001:2022 (ISMS)

Qatar National Information Assurance Policy V2 (NIAP)

Qatar Cybersecurity Framework (CSF)

March 2025

DOCUMENT OWNER

IT Director
Information Technology Services
Qatar University
P.O. Box 2713
Doha, Qatar

APPROVAL

	Prepared By	**Verified By**	**Approved By**
Name	Mohamad Eljazzar Divya Mohan	Thanzeer Hamarudeen IT Managers	Reem A. Al-Ansari
Title	Manager, IT GRC Senior Risk &Compliance Specialist	Section Head of Information Assurance	Director, Information Technology Services
Signature			
Date			1 February 2023

CHANGE HISTORY

Issue No.	**Date**	**Description of Change**
1.0	Dec 2013	Initial Draft
1.1	Sep 2014	Revised
2.0	Apr 2016	Major update to ITS policies. Incorporated all Information Security policies.
2.1	May 2017	Refinement Updates to address gaps identified by Deloitte
2.2	Aug 2017	Added several policies
2.3	Sep 2017	Review by IT Director
2.4	15 Oct 2017	Review by IT Management
2.5	23 Oct 2017	Incorporated IT Director and Managers' reviews Rearranged and renumbered policies
3.0	June 2018	Aligned with the NIA policy 2.0 Separated from IT policies
3.1	October 2018	Minor revisions, including comments from IT Director
3.11	November 2018	Corrected minor mistake (GS->SG), added "Policy" to each title
4.0	July 2019	Review of the policies
4.1	August 2019	1. Removed Acceptable Use Policy in favor of a more comprehensive one that is part of the IT Policies 2. General review and editorial changes
4.11	September 2020	General review
4.12	July 2021	1. Updated access control policy to include periodic access reviews. 2. Fixed some problems with numbering

5.0	February 2023	Major revision, including adding several new policies to be in line with the Qatar Cybersecurity Framework
5.1	September 2024	Review
5.2	March 2025	Review and updates to ISO27001:2022 Revised "Protection of Intellectual Property Policy"

DISTRIBUTION LIST

This document is maintained as a controlled document by the Information Security Manager and is available to all department employees as an uncontrolled document.

S/N	Position	Remarks
1	IT GRC Manager	Controlled
2	Others	Uncontrolled

1. OBJECTIVES

This document includes all information security-related policies that are designed comply with both ISO 27001:2013 (ISMS), the Qatar National Information Assurance Policy (NIAP), and the Qatar Cybersecurity Framework (QCSF).

2. SCOPE

The scope of this document includes policies listed below:

These policies act as a support guide to the Information Security Policy in order to perform processes in an efficient, streamlined and thorough manner and meet the objectives of the Information Security Policy.

Throughout this document, the term "**Information Security Manager**" (**ISM**) refers to the IT Services Department's designated person in charge of Information Security.

CONTENTS

PL-IS-02: Information Classification Policy

Contents:		
• Policy Description • Who Should Know This Policy • Purpose • Scope • Definitions • Policy • Procedures	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

Information classification is an important element of information security because it directs focus to where it is important. The information classification policy demands close cooperation between various business units and ITS in order to properly identify, control and protect QU information.

2. WHO SHOULD KNOW THIS POLICY

☒ President
☒ Vice President
☒ Office of the General Counsel
☒ Dean
☒ Director/Department Head
☒ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☒ Faculty
☒ Staff
☐ Student
☒ Third Party Users of QU Information Resources

3. PURPOSE

The purpose of this policy is to ensure that information receives an appropriate level of protection in accordance with its importance to the University. In addition, this policy provides a consistent framework for asset classification that is a fundamental requirement and a basic building block in the implementation of a sound information security policy.

4. DEFINITIONS

Term	Definition
Information Asset (“Asset”)	An information asset ("Asset") is defined as one of the following: • Electronic or other forms of information that are used to conduct a University business • Hardware, software, processes, and/or people utilized in the access, processing, transport, and/or storage of data as defined above
NIAP	Qatar National Information Assurance Policy
QCSF	Qatar Cybersecurity Framework (formerly known as the FIFA World Cup 2022 Cybersecurity Framework)
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Availability	Ensuring timely and reliable access to and use of information
Confidentiality Level	• C0 – Public • C1 – Internal • C2 – Limited Access • C3 – Restricted • C4+ – National Security Marking

5. SCOPE

The Information Classification Policy applies to all information assets that are handled, maintained, or operated by Qatar University or its associates in the course of conducting the University’s business.

6. POLICY STATEMENTS

Qatar University shall:

1. Classify information assets according to the Qatar National Data Classification Policy (NDCP).
2. Commit to implementing controls to protect the confidentiality of its users’ information.
3. Prioritize the implementation of controls based on the aggregate security level.
4. Implement the minimum appropriate set of baseline controls required to ensure the confidentiality, integrity, and availability of QU information assets. Additional controls may be implemented as deemed appropriate.
5. Consistently protect controlled information assets throughout their lifecycle in a manner commensurate with their sensitivity, regardless of where they reside, what form they take, what technology was used to handle them, or what purpose(s) they serve.
6. Ensure assets with confidentiality requirements are appropriately labelled.
7. Develop a compliance plan, which shows the compliance priority of processes, their dependent information assets and the schedule for assessment and control implementation.

8. Develop procedures and guidelines related to the labelling, handling, and destruction of classified information assets in line with the Qatar National Information Assurance Standard (NIAS).
9. Prioritize compliance with this policy by determining the criticality of ITS processes according to their criticality based on:
    a. Local laws and regulations
    b. QU policies and guidelines
10. This policy shall remain consistent with the NIA Standard or equivalent.

6.1 Performing Asset Classification

1. QU ITS shall identify the information assets and asset type
2. QU shall rate the information assets as High, Medium or Low, as outlined in the NDCP's data classification matrix.
3. per the compromise parameters i.e. Confidentiality, Integrity, Availability based on the data they process or store. The asset classification shall be based

Confidentiality

The confidentiality of information means access to the data is allowed only for authorized persons or technical means.

- C0: Public information. Classification label: "Public".
- C1: for internal use; material whose disclosure would cause light to moderate damage to the affected party.
- 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.).
- 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.).

Integrity

The integrity of data means the guarantee of the correctness, completeness, up-to-datedness and authenticity of data and absence of unauthorized alterations.

- I0: Source of information and time of changes are not important
- I1: It should be possible to identify the source of information and time of changes
- I2: Source of information and time of changes is identified and periodically checked
- I3: Authenticity and integrity should be provable to third party

Availability

The availability of data means timely and easy access to usable data during previously agreed necessary and required business hours (i.e. at the necessary and required moment and within the necessary and required period) for authorized persons or technical means.

- A0: Availability and productivity/reaction time not important
- A1: Availability 90% (downtime ~ 17h/week); allowed max response time – hours (1 to 10)
- A2: Availability 99% (downtime ~ 2h/week); allowed max response time – minutes (1 to 10)
- A3: Availability 99.9% (downtime ~ 10min/week); allowed max response time – sec (1 to 10)

Privacy

FUNCTION	LABEL			
	PUBLIC	**INTERNAL**	**RESTRICTED**	**SECRET**
Access	Open for all	Everyone in QU This can also include non-employees (contractor staff and consultants) officially working for QU IT	QU employees and contractors who have signed non-disclosure agreements and who have a business need to know	QU employees and contractors who have signed non-disclosure agreements and who have a business need to know. Access to contractors will be given only after due risk assessment.
Electronic Distribution	No restrictions	No restrictions on data transfer but should be sent only to the approved recipients	No restrictions on data transfer but should be sent only to the approved recipients	Should be sent only to the approved recipients and it is recommended that all information be encrypted if it is sent over public network
Storage	No security controls required	Baseline security controls to ensure no access to users outside of QU .	Electronic data should have individual access controls where possible and appropriate	Individual access controls are MUST for the information in electronic form. Storage device should have necessary physical as well as logical security
Disposal	No security controls required	Electronic data should be erased. Need to ensure that it is not left in the recycle bin. Paper assets should be properly torn into small pieces rather than just crumbling. Removable storage media to be physical destroyed if not re-usable.	Electronic data should be erased. Need to ensure that it is not left in the recycle bin. Paper assets should be properly torn into small pieces rather than just crumbling. Removable storage media to be physical destroyed if not re-usable.	As far as possible, electronic data should be reliably erased using appropriate software utility rather than just the delete functionality provided by the operating system. Removable storage media to be physically destroyed if not re-usable. Paper assets should be shredded.

6.2 Information Labeling, Handling and Storage

Labeling

- QU shall mark all the assets, records and media (paper, electronic or otherwise) containing sensitive or internal information as INTERNAL, RESTRICTED or SECRET with those words in prominent places such as, headers, footers, title pages, stamps, labels, or other markings, as suitable for the media used. However, the lack of such appropriate marking shall not be deemed conclusive that the information may be handled as PUBLIC.
- There are no restrictions on information sharing when the information is to be shared with government, legal, judiciary, statutory or regulatory authorities.
- Information sharing with external auditors for quality, information security and finance is permitted.
- Confidential information shall not be distributed (within or outside the organization) in any manner (including any form of media) without proper authorization from Management.

- Restricted information shall be provided only to organizational members on “Need to Know” basis. If there is need to share such information to any outsider, it shall be shared only after signing “Non-disclosure” agreement.
- Interviews to publicity media, publication of any article in media, participation in any public / social events where there is likelihood of sharing company related information must be done with prior authorization from Management. However, no sensitive information shall be disclosed in such events. It must be ensured that the dissipated information to publicity media does not get distorted which may affect organizational image. Records of such publications must be maintained.

Information Storage

RESTRICTED/SECRET information shall be secured by applying appropriate security controls.

Information in transit

If there is need to send RESTRICTED or SECRET information outside the organization, it would be sent by using trusted encryption mechanisms or by courier service. The recipient’s name shall be clearly mentioned on the envelope and receipt acknowledgement shall be obtained.

6.3 Declassification

Data declassification can be done either by the owner or by the University if the information is no longer restricted, limited Access or internal. While defining the information classification the owner should define the time period for which the information can be considered as classified information.

6.4 Information Disposal

1. QU shall physically destroy confidential information in paper / hard copy format, e.g. through secure shredding.
2. QU shall implement techniques like demagnetizing, degaussing or overwriting media having restricted or secret information on electronic media.

PL-IS-03: Protection of Intellectual Property Policy

Contents:	Version Number:	6
• Policy Description • Who Should Know This Policy • Overview • Scope • Policy • Policy Sections	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses the importance of preserving and protecting the intellectual property at Qatar University.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to protect the intellectual rights with regard to IT resources in use at Qatar University.

4. SCOPE

This policy addresses intellectual property rights of third party organizations, such as software and IT systems and digital resources.

5. POLICY STATEMENTS

Qatar University is committed to compliance with intellectual property rights of third parties, including but limited to software and other digital material.

1. QU shall acquire software only through trusted and vetted sources to ensure copyright is not violated.
2. QU shall maintain a software asset register with proof of ownership of software licenses, right to use, and other documentation that can assert the University's ownership or right of use.
3. Internal audits shall be conducted to ensure compliance.
4. Users shall not install or use unlicensed software on QU information systems or networks.
5. IT Services staff shall report observed breaches to the IT Director.
6. Qatar University prohibits the use of its computers, networks, or other technology resources for the purpose of illegally sharing copyrighted material.
7. Users are prohibited from using QU devices and IT infrastructure and network to illegally access, use, copy, reproduce, or make available copyrighted materials to others.
8. QU users shall use software in accordance with the terms and conditions of the license agreements.
9. Users implicated in copyright violations will be subject to disciplinary action as per QU policies and local laws and regulations.
10. Users will need to obtain appropriate permission to distribute protected material including text, photographic images, audio, video, graphic illustrations, and computer software.
11. Users may not use QU IT systems or devices to violate the ethical and legal rights of any person or company protected by copyright. These violations include, but are not limited to:
    a. Unauthorized copying, distribution, display or publishing of copyright material. These include but are not limited to digital imaging for the purpose of distribution of photographs from magazines, books, copyrighted music, and copyrighted video.
    b. Displaying and/or publishing licensed material without proper authorization from the owner.
    c. Breaching confidentiality agreements that QU may have with software/services providers.
    d. Using QU electronic devices and equipment for any act of academic dishonesty as prohibited by the University (such as plagiarism)

6. ROLES AND RESPONSIBILITIES

1. All users of QU IT resources are responsible for adherence to this policy.

2. QU business units are responsible for enforcing this policy among their employees.
3. The Information Security Manager is responsible for audits, compliance, and enforcement of the policy.
4. The QU Office of the General Counsel is responsible for handling any and all reported cases where intellectual property rights may be breached.

7. COMPLIANCE

Failure to comply with this policy may result in disciplinary action as per QU regulations and/or local laws and regulations.

8. EXCEPTIONS

There are no exceptions to this policy.

PL-IS-SG-01: Information Security Governance Structure

Contents: • Policy Description • Who Should Know This Policy • Scope • Policy • Roles & Responsibilities	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The Information Security Governance policy establishes the foundation for managing the information security program at Qatar University. It also addresses some of the activities necessary to ensure that security is maintained.

2. WHO SHOULD KNOW THIS POLICY

☒ President
☒ Vice President
☒ Office of the General Counsel
☒ Dean
☒ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to define the governance structure for managing information security at Qatar University.

4. POLICY STATEMENTS

Qatar University is committed to ensuring the proper management and security of its information assets in accordance with established best practices, and in compliance with all relevant laws and regulations. In particular, the University shall keep the Qatar National Information Assurance Policy (NIAP) in focus as it develops its information security and assurance strategy.

In that regard:

1. Qatar University's senior management shall be the highest approval authority for all policies and strategic plans related to information security.
2. Qatar University shall establish a steering committee to address the organization's information security issues and provide guidance for the proper management of information assets. This committee shall include representatives from various academic, research, administrative, and technology fields.
3. Qatar University shall comply with the minimum requirements of the Qatar National Information Assurance Policy's Governance Structure with regard to management of the Information Security program. This includes the appointment of "a person to own and manage the information security program" (hereunto referred to as "Information Security Manager" or "ISM").
4. The ISM is responsible for the development, oversight, and implementation of all information security related processes at all QU managed and operated locations and venues. In addition, the ISM shall ensure the proper handling of QU information by third parties through oversight and constant monitoring and review.
5. The IT Services department is responsible for the development and implementation of IT security policies and controls that are mandated by any adopted security management framework (e.g. ISO 27001 or the NIA policy).
6. Key QU business sectors shall identify at least one person to act as a liaison with the ISM. This "information security liaison" shall be well versed with the major functions of the business unit, in particular with respect to the nature and flow of information within the business unit.
7. Information owners shall be responsible for the identification, proper classification of their information asset. They are also responsible for defining proper access authorization levels to their institutional data.
8. Information custodians shall be responsible for implementing controls identified and recommended by the Information Security Manager.

5. SECURITY GOVERNANCE ROLES AND RESPONSIBILITIES

1. All QU constituents are expected to fully cooperate with the Information Security Manager to ensure the confidentiality, integrity, and availability of QU information assets.
2. The QU Executive Management Committee (EMC) shall:
    a. Provide the required support, insight, guidance, and general input with regards to QU strategy as it relates to information assurance.

b. Ensure the support of various business units for various information assurance initiatives.
c. Be responsible for the promulgation of information security policies.

3. The Information Security Steering Committee's role is to validate and promote the recommendations of the Information Security Manager's leading role in the information assurance process. The Committee's role is critical in:
   d. The establishment and ratification of information security policies, guidelines, and standards.
   e. Monitoring of guidelines to ensure that QU personnel adhere to the Information security policies.
   f. The promotion of information security awareness and its importance to the University.
4. The Information Security Manager (ISM) shall work with the various groups on campus to assure the appropriate levels of confidentiality, integrity, and availability of information assets to the respective stakeholders. The ISM shall:
   a. Identify, develop, and produce the necessarily policies, guidelines, standards, and other documents needed to assure the appropriate levels of confidentiality, integrity, and availability (C.I.A.) of information assets.
   b. Respond to and manage exceptions to information security-related policies.
   c. Establish and maintain compliance with relevant laws, regulations, standards, and generally-accepted best practices as they relate to information assurance.
   d. Ensure that QU's information security policies comply with the Qatar National Information Assurance Policy or its equivalent.
   e. Embrace a risk-based information security management program that identifies risks associated with the management of QU information assets and proposes corresponding risk management strategies.
   f. Have sufficient resources to execute the assigned tasks.
   g. Provide ITS management with audit reports of their critical system components and ensure that corrective actions have been taken.
   h. Be directly responsible for ensuring that all QU personnel are aware of their obligations to safeguard the University's information assets.
   i. Enforce the implementation of information security policies.
5. The IT Services department plays a key role security QU institutional data. The department shall:
   a. Lead all IT security efforts on campus
   b. Commit the necessary resources to manage the information security management system.
   c. Foster an environment where security is always included as a fundamental component of IT service delivery and operations.
6. Critical business and technical units shall be identified and requested to appoint at least one Information Security Liaison to act as the single point of contact for the ISM within the unit. The Information Security Liaison shall:
   a. Be well-versed with the business conducted within the business unit, in particular with regard to the flow and handling of information.
   b. Assist the ISM in data classification, process analysis, and risk assessment efforts necessary to implement a risk-based security management framework.

   c. Inform the business unit of relevant information security efforts, policies, and guidelines.
   d. Ensure that business unit's input is communicated to, and considered by the ISM.

7. Information owners are expected to:
   a. Be able to assert their ownership of their data
   b. Define and maintain information assurance profiles for their information and related processes, e.g. classification, access control, handling guidelines, chain of authority, etc.
   c. Report any breaches or attempts at compromising their information to the appropriate authority.
8. Information custodians are expected to:
   a. Be able to identify the owners of the data with which they are entrusted.
   b. Implement and maintain the required baseline controls necessary to protect the data per the QU information security policies and guidelines.
   c. Report any breaches or attempts at compromising the information under their custody to the appropriate authority.
9. Information Users must:
   a. Comply with all policies approved by Qatar University.
   b. Ensure that information and data are solely used for purposes specified by the resource owner/custodian.
   c. Ensure that QU's information resources are maintained and utilized in the most efficient way possible and they are used for legitimate business purposes only.

PL-IS-SG-02: Risk Management Policy

Contents:		
• Policy Description • Who Should Know This Policy • Purpose • Scope • Definitions • Policy • Policy Sections	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

Risk management is at the core of all information security efforts and is required by the frameworks adopted by the Information Technology Services department, namely ISO 27001 and the Qatar National Information Assurance Policy (NIAP). This policy focuses on risk management as a fundamental approach to information security management.

2. WHO SHOULD KNOW THIS POLICY

☒ President

☒ Vice President

☒ Office of the General Counsel

☐ Dean
☐ Director/Department Head
☒ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student

☒ Third Party Users of QU Information Resources

☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to establish risk management as the foundational building block for information security at QU. The implementation of this policy should help maximize opportunities, minimize adversity, and effectively manage the risks associated with the delivery of critical IT services and functions based on informed decision-making and organizational resilience.

4. SCOPE

This policy applies to all QU information assets.

5. DEFINITIONS

Term	Definition
Risk	The effect of uncertainty on objectives. The effect is a positive or negative deviation from what is expected.
Risk Management	Refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the University.
Risk Assessment	Consists of identifying and assessing risks that can potentially disrupt business operations.

6. POLICY STATEMENTS

The Information Technology Services department is committed to ensuring that effective risk management remains central to all its operations while delivering its services to the University.

ITS shall:

1. Define a risk assessment process to identify threats and vulnerabilities to critical information assets.
2. Prioritize the identified risks based on their criticality.
3. Based on the assessment, define a risk treatment plan to address the identified threats and vulnerabilities.
4. Ensure that senior management vets the risk treatment plan and residual risk for information assets that carry a high level of risk.
5. Monitor and evaluate selected risk treatment controls on a regular basis to ensure their continuity and effectiveness.
6. Endeavour to embed risk assessments into the design and review of business processes, policies, processes and procedures and are followed through in project lifecycles.
7. Conduct periodic reviews and re-assessment of risks to ensure that they do not creep into projects or operations.

The risk management framework shall reflect good practice and sound corporate governance and be consistent established standards or frameworks.

PL-IS-SG-03: Third Party Security Management Policy

Contents:	Version Number:	5
• Policy Description • Who Should Know This Policy • Introduction • Policy • Policy Sections	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

Engagements with third party suppliers introduce risks associated with access of the suppliers' personnel or systems to QU IT information resources. In addition, business continuity for QU processes can be at risk of partial or complete disruption in case a supplier fails to provide proper controls to ensure service continuity. This policy addresses this issue.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☒ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure the proper governance of relationships with third parties in order to ensure that any potential risks are assessed and appropriate mitigating controls are implemented.

4. SCOPE

This policy applies to all IT supplier engagements with Qatar University, in particular when suppliers have access to QU computing systems, applications, network, files and other information resources.

5. DEFINITIONS

Term	Definition
QU IT Resources	QU network, system(s), computing device(s), and electronic information.
Third Party	Any non-QU entity that that requires access to QU IT resources during its engagement with a QU Unit (see below). This includes, but is not limited to, vendors, service providers, consultants, external researchers, partners and other non-QU entities.

6. POLICY STATEMENTS

The Information Technology Services Department shall ensure compliance with the National Information Assurance Policy and ISO27001:2022with regard to the Third Party Security Management. Namely, the department shall ensure that:

1. All relevant information security requirements are identified and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for Qatar University.
2. Supplier agreements are established and clearly and unambiguously documented.
3. Requirements to address the potential or identified information security risks associated with information and communications technology services and product supply chain are included on the agreements with suppliers.
4. Any change in service provider shall have proper approval. If required, reassessment of the risks shall be done considering the criticality of the services.
5. Information security controls are identified and mandated.
6. The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services are considered in the agreement to avoid any delay in arranging replacement products or services.
7. An agreed upon level of information security and service delivery is defined and is in line with supplier agreements.
8. Monitoring, review and audit of supplier service delivery are conducted regularly.
9. A service management relationship process between ITS and suppliers is defined and assigned to a designated individual or service management team.
10. Appropriate actions are taken when deficiencies in the service delivery are observed.
11. The department retains visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.
12. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account

of the criticality of business information, systems and processes involved and re-assessment of risks.

13. Third parties who require access to QU infrastructure or information assets are bound by a contract that defines QU's security requirements. Prior to being granted any access, they are required to sign a non-disclosure agreement.
14. Proper training should be carried for third party users of the service in methods, procedures and security where applicable, e.g. Security Personnel.

7. RESPONSIBILITIES

Responsibilities towards this policy shall be clearly identified in procedure document:

1. For enforcing the policy and ensuring its implementation, in addition to the continuous review of the policy to ensure its validity over time.
2. Support and commitment towards ensuring of the implementation of this policy.
3. Ensure compliance with this policy.

PL-IS-SG-04: Data Labelling Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses the requirements for labelling information assets per their classification level to ensure the designated users of information assets will be able to correctly identify and adequately allocate resources for their protection.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☒ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☒ Faculty
☒ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

This policy provides a high-level data labelling methodology for the purpose of understanding and managing data and information assets with regard to their level of classification. The policy explains the methodology and the processes for effective data labelling.

4. SCOPE

All institutional data.

5. POLICY STATEMENTS

To meet the requirements of this policy, QU must:

1. Serve as a labelling authority for the data and information that it collects or maintains.
2. Rate all information assets in accordance with the data classification standard. All assets rated with a confidentiality rating of C1, C2 or C3 shall suitably mark the data label of Internal, Limited Access or Restricted respectively.
3. By default, classify information assets as “Internal” unless they are specifically for public release or consumption.
4. Establish the data labelling system to support the “need-to-know” requirement, so that information will be protected from unauthorized disclosure and use.
5. Establish data labelling education and awareness for staff, employees and contractors.

6. EXCEPTIONS

Information assets that cannot be easily labelled should be documented in an alternate manner.

PL-IS-SG-05: Change and Patch Management Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

Uncontrolled changes to IT systems and services can result in major disruptions and result in loss of productivity for students, faculty and staff. A change management policy is essential to assure that all changes that may impact users are planned and executed in a controlled manner.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure that changes to IT systems and services are managed in a rational and predictable manner. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

4. DEFINITIONS

Term	Definition
Change	A change to an IT resource such as an operating system, IT hardware, network, software, or service
Urgent Change	A change that must be implemented within a short period of time, e.g. 24 hours.
Emergency Change	A change that must be implemented as soon as possible to recover from an outage.

5. SCOPE

Any change that might affect the IT resources upon which University personnel rely to conduct normal business operations is within the scope of this policy. The following non-exhaustive list illustrates common types of change:

1. Software upgrades, updates or additions
2. IT infrastructure changes
3. Preventative maintenance
4. Security patches
5. System architecture and configuration changes
6. Hardware upgrades

This policy applies to all the individuals who install, operate or maintain information technology resources.

6. POLICY STATEMENTS

The IT Services department shall establish and activate a formal change management process to ensure that changes to IT systems and services are conducted in a controlled manner.

1. Planned changes shall be implemented at times where there is minimal or no negative impact on user services.
2. The process shall embed proper authorization levels to ensure transparency.
3. Communication with the appropriate stakeholders shall be an essential component of all major changes.
4. The change management process shall include provisions for handling urgent and emergency changes in order to avoid further degradation or disruption of services.
5. ITS shall encompass the following changes in the information and IT environment but not limited to:
    a. Assessment of probable impact of such changes on business and on security
    b. Implementation of new resource / functionality
    c. Modification of existing resources

d. Removal or disposal of existing resource

6. QU shall:

a. Form a Change Advisory Board, which must include representation from security and risk divisions and/or from various business /functional units.

b. Define and implement Change impact and risk criteria for all the changes, configurations and patches on all the information assets.

c. Define a rollback/recovery procedure to restore from undesired outcomes.

d. Conduct vulnerability scanning of critical systems at least once in a year/on-periodic basis.

e. Download all patches from the relevant system vendor or other trusted sources. Each patch's source must be authenticated and the integrity of the patch verified. All patches must be submitted to an anti-virus scan upon download.

f. Assess any change be authorized by ISM who assesses the business, financial, technical and regulatory impact of all major changes.

g. Ensure that all changes and patches are tested prior to their release in the environment.

h. Define a process to detect, alert, investigate and notify relevant stakeholders from unauthorized changes.

i. Maintain a separate development, test and operational environments to protect from unauthorized access or change to the information assets.

j. Ensure Emergency changes require verbal/informed approval from Change Manager and business owner (if required). However, formal documentation and risk analysis shall be performed after the emergency.

k. Apply patches according to the patching schedule causing minimal disruption to business:

l. Update Change Management Database and all configuration and inventory documentation upon any change and patch deployment respectively.

m. Conduct periodic audits to ensure that patches have been applied as required and are functioning as expected.

n. Ensure to establish and maintain a secure channel to communicate, agree, and approve service outage and business outage resulting from change, configuration, and patch deployment activities within the change control committee.

o. Establish a process to notify internal and external entities for planned and unplanned outages.

p. Define escalation mechanisms and actions plans in the event of security breaches/unauthorized changes that include communicating to Internal and external entities.

q. Ensure changes, patches, and configuration changes are properly categorized and prioritized based on business / security requirement.

PL-IS-SG-06: Personnel Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

"People – Process – Technology" is the golden triangle necessary for a strong information security foundation. The "People" element is usually cited as the weakest and most risky, which necessitates that organizations such as Qatar University thoroughly vet potential employees who will have access to confidential information.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☒ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☒ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☒ Faculty
☒ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure that QU personnel are aware of their security responsibilities and that suitable controls are in place to mitigate risks arising out of the human element.

4. SCOPE

This policy applies to all individuals employed by Qatar University and who have access to non-public institutional information.

5. POLICY[1]

Qatar University shall maintain compliance with the National Information Assurance Policy with regard to personnel security. Namely, the University must, at a minimum:

1. Ensure that the Human Resources processes are aligned with information security policies and initiatives for Qatar University.
2. Ensure the HR department documents security requirements, obligations, and ways of working in HR manual, which is read, understood and available to all staff to ensure they are aware and comply with their obligations to information security.
3. Obtain, manage and retain information related to personnel with due care and due diligence, in line with the requirements for handling personal information.
4. Conduct adequate screening to ascertain the integrity of prospective candidates for employment and contractors (including sub-contracted workers).
5. Ensure that staff sign an agreement, on joining the University or when there is a change in job profile or duties, which outlines their security obligations and responsibilities.
6. Define, communicate and enforce a disciplinary process and ensure that employees are made aware of the process.
7. Ensure that vendors, contractors, delegates or guests visiting ITS premises are properly escorted and their presence managed.
8. Ensure that a change request from the HR department is generated when a change of duties or termination of contract of an employee, contractor or third party occurs.

[1] Adapted from the Qatar National Information Assurance Policy 2.0

PL-IS-SG-07: Security Awareness Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The purpose of this policy is to define criteria for a security awareness and training program

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☒ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to define criteria for a security awareness and training program conducted by the University for its employees, students, contractors, temporary personnel, and other entities who may use or administer the University's information system assets.

4. SCOPE

All users of QU information resources.

5. POLICY STATEMENTS

To meet the requirements of this policy, Qatar University must ensure:

1. A security awareness program is defined and adequate budgets are allocated for this implementation.
2. As a minimum, such training includes:
    a. Qatar University's security requirements
    b. Legal and regulatory responsibilities
    c. Business-specific processes and controls
    d. Acceptable use of IT resources
    e. Information on the enforcement and disciplinary process
    f. Information on who to contact for further security advice and the proper channels for reporting information security incidents
3. All QU users and, where relevant, contractors an third party users receive appropriate security awareness training regarding the University's policies and procedures, as relevant for their job function, roles, responsibilities and skills.
4. Users should be trained to recognize social engineering attempts on them and not disclose any information that could violate the University's security policies, such as during social gatherings, public events and training events.
5. Contents of the security training and awareness are reviewed and updated regularly to reflect new trends, new threats, and changes to the University's information technology infrastructure or applicable laws and regulations.
6. New employees are provided information security awareness training as part of the employee induction process and refresher training must be conducted on periodic basis.
7. Training is followed up with an assessment, to ascertain the effectiveness of the program, including maintaining of records of attendance of security awareness programs.
8. Indirect media such as posters, intranet, email, etc. may be used effectively to support the awareness program.

PL-IS-SG-08: Incident Management Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The Information technology Services Department is committed to ensuring its ability to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable and predefined level. This requires that we identify the threats to our organization and the potential impact those threats may have on our operations.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

This policy intends to provide a reference for the Agency's management, administration and other technical and operational staff to facilitate the development of information security incident management capability, and to be used for preparation for, detection of and response to information security incidents.

4. SCOPE

All security incidents related to QU and QU information assets.

5. POLICY STATEMENTS

To meet the requirements of this policy, Qatar University must:

1. Appoint a person to own and manage the Incident Management program, including a point of contact for all information security communications.
2. Establish an information security incident response capability which is capable of making a periodic risk assessment (from threat, vulnerability and asset value) of data, processes, systems and networks.
3. Define procedures to detect, evaluate and respond to incidents.
4. Define procedures to report, manage and recover from information security incidents, internally, with local authorities.
5. Create awareness amongst its staff to report incidents.
6. Categorize and prioritize all incidents according to a predefined incident criticality classification.
7. Co-ordinate with local authorities to create a repository of incidents in the University.
8. Report all Criticality Level 1 incidents to the local authorities within one (1) hour of identification.
9. The Incident Management coordinator is responsible for developing and executing an annual Security Assurance Plan. This may include activities such as penetration testing, audit of security procedures, and incident scenario testing.

5.1 Preparation

QU shall:

- Establish formal incident handling and response policies and procedures.
- Establish governance and define incident handling and response roles and responsibilities.
- Deploy and train team members to support?
- Prepare Incident Response Contact List which should include contact information (phone numbers, mobile numbers, emergency contact numbers, email addresses, public keys etc.) of all internal and external stakeholders.
- Protect Incident Response communication.
- Ensure security risks identified for the infrastructure, endpoints and applications during the risk assessment have been communicated team responsible for 'Incident Handling and Response'.
- Implement out-of-band communication channel in the event normal communication channels are compromised.

- Test response plan with critical suppliers/providers.
- Ensure that the incident management coordinators develop and execute annual test plan that simulates how ITS shall respond to information security incident.
- Ensure that the Incident Management process owner (IM Manager) assesses the requirements for the Incident response capability in context of the organization's business requirements.

5.2 Detection and Analysis:

ITS shall:

- Ensure that any security breach or weakness observed in the security arrangements that challenge or compromise the security arrangements of ITS is reported immediately to the Incident Response Manager.
- Once the incident/weakness is identified, raise a security incident by sending an email/call/other suitable means of communication to Security/Helpdesk team.
- Ensure that Incidents are categorized and assigned an appropriate criticality level/classification consistent with response plans
- Perform forensics if required after getting authorization approval from the management.
- Establish processes to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources

5.3 Containment, Eradication and Recovery

- ITS shall contain and mitigate incident in a timely manner.
- Information security incidents shall be responded to in accordance with the documented procedures.
- Specific incidents of a more serious nature or with a potential for further negative impact on QU shall be addressed specifically with the top management.

5.4 Post Incident Activity

- Knowledge gained from analyzing and resolving information security incidents shall be used
- Where a follow-up action against a person or organization after an information security incident involves a legal action, evidence shall be collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction by ISM.
- Appropriate disciplinary action shall be taken against a person believed to have been intentionally involved in the security incident.
- ITS shall take appropriate corrective and preventive action to reduce / eliminate occurrences of such incidents.

5.5 Forensic Analysis

- Organization shall define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence.

PL-IS-SG-09: Business Continuity/Disaster Recovery Management Policy

Contents:	Version Number:	4
• Policy Description • Who Should Know This Policy • Policy • Policy Sections	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The Information technology Services Department is committed to ensuring its ability to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable and predefined level. This requires that we identify the threats to our organization and the potential impact those threats may have on our operations.

2. WHO SHOULD KNOW THIS POLICY

☒ President
☒ Vice President
☐ Office of the General Counsel
☐ Dean
☒ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to assert the requirement to establish a business continuity management system (**BCMS**) that addresses the requirements for business continuity for ITS.

4. SCOPE

The Business Continuity requirements set forth in this policy apply to the IT Services Department.

5. DEFINITIONS

Term	Definition
Disaster	An unexpected disruption to normal business of sufficient duration to cause unacceptable loss to the organization necessitating disaster recovery procedures to be activated.
Disaster Recovery (DR)	Activities and procedures designed to return the organization to an acceptable condition following a disaster.
Business Continuity (BC)	The uninterrupted availability of all key resources supporting essential business functions.
Business Continuity Management	Provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives.
Business Continuity Planning	A process developed to ensure continuation of essential business operations at an acceptable level during and following a disaster.
RTO - Recovery Time Objective	The targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
RPO - Recovery Point Objective	The maximum acceptable amount of data loss measured in time.

6. POLICY STATEMENTS

The IT Services Department shall develop and implement a comprehensive business continuity plan to enable it to recover, operate and support essential QU business processes and IT services.

In order to comply with this policy, the department must ensure:

1. A Business Continuity (BC) Plan is prepared to ensure continuance of critical processes and the delivery of essential services to an acceptable level. This plan SHALL include, and be based on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each ITS process and service.
2. The BC Plan covers potential disaster scenarios and includes disaster recovery provisions.
3. The BC Plan is maintained and updated to reflect the current status and requirements and relevant information is made available for all team members, employees and service providers.
4. A copy of the up to date BC Plan along with the necessary backup data tapes media and information is stored in a fire/tamper proof safe, along with an additional copy stored in an off-site location, preferably in a geographically different one than the primary data center.
5. The identification of alternate disaster recovery sites, whose readiness is determined by the RTO requirements. These sites may be Hot/Warm/Cold Sites depending upon the University's requirements.

6. Strong controls are specified in contracts that involve outsourcing a portion of the business or information technology functions or business continuity services.
7. The BC Plan is periodically tested at least on an annual basis or when significant changes take place in the business or legal/regulatory requirements.
8. Awareness about the BC plan is created amongst QU employees.

6.1 Establish

QU shall:

- Design a recovery capability that enables it to promptly and effectively respond to cybersecurity disruption's and maintain continuity of its prioritized IT/OT activities, considering all interested parties involved in performing prioritized activities.
- Establish a governance model to oversee the management of the recovery and continuity program at the entity, with detailed roles and responsibilities.
- Identify relevant legal and regulatory framework as set by international, national and sector level standards, legislation and practices for mandatory compliance.

6.2 Operations

- QU shall define methodology and process for conducting Business Impact Analysis (BIA) and Threat and Risk Assessment, using a combination of qualitative and quantitative metric and indicators.
- QU shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations
- Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
- The Business Continuity Plan shall anticipate various business disruption scenarios; whether mild or severe and incorporate protection accordingly.
- ITS shall specify information security controls in a third-party contract that involve outsourcing of any service/business function.
- The Business Continuity Plan shall be tested on periodic basis or upon any major change takes place in the business or legal/regulatory requirements.
- QU shall maintain emergency / crisis communication guidelines with protocols and requirements for effective internal / external communication with key stakeholders, government agencies / interested parties and customers.
- QU shall stimulate a culture of recovery and continuity across the entity and sector through regular awareness programs, communications and training.

6.3 Review

- ITS shall evaluate and identify the improvements of recovery and continuity capability. These review's and updates are obligatory when a change takes place in the entity.

6.4 Improvements

- QU shall ensure recovery and continuity capability are valid and consistent with the National and Entity cyber resilience objectives.
- QU shall review of recovery and Continuity program against established Performance matrices and key performance indicators.

PL-IS-SG-10: System Logging and Security Monitoring Policy

Contents:	Version Number:	5
• Policy Description • Who Should Know This Policy • Policy • Policy Sections	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The policy is defined to set forth the minimum requirements for logging and monitoring activities that needs to be carried out with in Qatar University IT infrastructure.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to provide requirements for logging and monitoring to identify unauthorized data, application and resource access and to detect unauthorized changes or access privileges abuse.

4. DEFINITIONS

Security Log	A log that contains records of login/logout activity or other security-related events specified by the system's audit policy.

Audit Log	A document that records an event in an information (IT) technology system. In addition to documenting what resources were accessed, audit log entries usually include destination and source addresses, a timestamp and user login information

5. POLICY STATEMENTS

ITS shall maintain compliance with the National Information Assurance Policy with regard to Logging and Security Monitoring policy. In order to comply with the NIA Policy, the University must ensure that[1]:

1. An adequate set of technical control implementations, or processes exists for logging, identification and continuous monitoring of access, changes, and command execution to, any/all information assets for protection of business sensitive information.
2. Monitoring practices are established in accordance with criticality of the infrastructure, data, and applications.
3. Logging is enabled on all infrastructure and data processing equipment, and applications that are associated with the access, transmission, processing, security, storage, and/or handing of information classified with a confidentiality rating of C2 (Limited Access) and above.
4. These logs are retained for a minimum of ninety (90) days and a maximum depending on criticality assessments and sector specific laws and regulations.
5. Audit logging or log capture are enabled to record date, time, authentication activity with unique user and system identifiers, including all failure or change actions, further including commands issued and output generated to provide enough information to permit reconstruction of incidents and move system to its original state.
6. Exceptions are identified and reported in accordance with the Incident Handling policy.

5.1 Audit Logging

Audit logging shall be implemented for all critical information systems including servers, network equipment, applications, personnel activity, external service provider and physical environment of QU and shall be reviewed on periodic basis.

5.2 Event Generation:

- ITS shall configure system to generate a success or failure event whenever:
    - server receives a bad/invalid logon request (account logon events)
    - a user account or group is created, renamed, changed or deleted (account management)
    - a user makes high-level changes to the security policies (policy changes)
    - whenever a user makes use of certain root or administrative privileges that are assigned by administrator (privilege use)
    - event whenever an event, which affects the entire system, occurs (system event)
- Organization shall communicate event detection information to appropriate parties.

[1] Reference: Qatar National Information Assurance Policy 2.0

5.3 Review of Operating Systems Log Procedure

Any additions, modifications or deletions of user accounts shall be reviewed for:

- Any failed or unauthorized attempt at user logon.
- Any modification to system files.
- Any access to the server, or application running on the server
- Actions taken by any individual with Administrative privileges.
- Any user access to audit trails.
- Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain System Administrator access to system)

5.4 Review of CCTV Log Procedure

- Any suspicious activity in the ITS premises
- Visitors without Badge in the ITS premises

5.5 Review of Antivirus Log Procedure

- Alerts generated by antivirus software
- Quarantine folder/ files
- White list of folders

5.6 Review of Cloud Server Logs

- Any failed or unauthorized attempt at user logon.
- Any access to the server, or application running on the server

6. EXCEPTIONS

Exceptions to this policy shall be assessed by Information Security Manager and require approval of the IT Director. Adequate controls shall be implemented to mitigate risk identified by not following the policy.

PL-IS-SG-11: Data Backup, Data Retention and Archival Policy

Contents:	Version Number:	4
• Policy Description • Who Should Know This Policy • Policy • Policy Sections	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses data retention and archival of QU institutional data. The Information Technology Services department is committed to ensuring its ability to plan for data backup, recovery, retention, and archival in order to respond to business disruptions in order to continue business operations at an acceptable predefined level.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to define the Information Technology Services' requirements for the backup of information, software and systems and to define the associated retention and protection requirements.

4. SCOPE

This policy applies to the backup of systems, applications, databases and user data placed under ITS custody.

5. POLICY STATEMENTS

The IT Services Department shall ensure that:

1. Backup copies of data, software and systems are taken and tested regularly and repeatedly.
2. Adequate backup facilities are provided to ensure that all essential data and software can be recovered following a disaster or system failure.
3. Processes for backup, archival and recovery of data have corresponding procedures which ensure that the integrity and confidentiality of the data is retained and that the backups are successfully executed as per the set policy and plan.
4. Removable backup media are stored in a fire and tamper proof cabinets, in addition to copies stored off-site at a location that is in a geographically different zone than the primary data center.
5. Backup media are encrypted where required.
6. Credentials of system administrators are backed up and safeguarded.
7. The retention period for essential business information is identified, considering any requirement for archive copies to be permanently retained. The data retention and archival shall comply with legal, regulatory and/or University policies and requirements.
8. Data which needs to be retained is stored ensuring confidentiality, integrity and availability and that it can be accessed for defined future purposes.
9. Personal and sensitive Information is not retained for longer than it is necessary as per the Personal Data and Privacy Protection Law.
10. Processes for backup, archival and recovery of data have corresponding procedures which ensure that the integrity and confidentiality of the data is retained.
11. Archived data retains it classification markings and is secured accordingly.
12. The archiving technology deployed is regularly reviewed to ensure that it does not suffer from obsolescence and archived data is maintained in a state that allows successful recovery.
13. The IT Services Department shall maintain a document that includes all details related to data backup, retention and archival, including but not limited to:
    a. Types of data
    b. Location
    c. Frequency
    d. Retention Period
14. Backup shall be tested for data integrity and reliability on a periodic basis.

15. ITS shall have in place an authorized people to accept/deny data restore request ticket (e.g. data owner, management).

6. RESPONSIBILITIES

Responsibilities towards this policy shall be clearly identified in procedure document:

1. For enforcing the policy and ensuring its implementation, in addition to the continuous review of the policy to ensure its validity over time.
2. Support and commitment towards ensuring of the implementation of this policy.

PL-IS-SG-12: Documentation Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

QU is committed to document information required by the ISO 27001 Information Security Management System standard and as required for its daily operations and management needs.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The main purpose of this policy is to outline the Information Technology Services' approach to documentation.

4. DEFINITIONS

Documentation set	A group of related documents (policies, processes, procedures, plans, guidelines, records, templates etc.) that can be created in one step and then managed as a single entity.

5. SCOPE

The documentation requirements set forth in this policy apply to ITS. It is relevant to all staff of Information Technology Services at Qatar University.

6. POLICY STATEMENTS

The IT Services Department shall ensure that:

1. Every system that is determined to be critical to the University is covered by a system security plan/standard. The University SHOULD ensure that, where necessary, security operating procedures are created and documented.
2. System security standards and procedures are aligned and consistent with the University's security policies and objectives.
3. Document sets are:
    a. available and suitable for use, where and when they are needed;
    b. adequately protected from authorized disclosure, improper use, or loss of integrity.
    c. controlled in terms of:
        i. distribution, access, retrieval and use;
        ii. storage and preservation, including the preservation of legibility;
        iii. control of changes (e.g. version control); and
        iv. retention and disposition.
    d. stored in a central repository with appropriate access controls.
    e. updated on the completion of each change and that old document sets are archived or disposed of; taking into consideration the requirements of the classification policy.
4. Information is documented and transferred to the University in cases where an employee or external party user has knowledge that is important to ongoing operations.
5. Documented information of external origin, determined by the University to be necessary for the planning and operation of the information security management system along with other daily operations, are identified and controlled as appropriate.
6. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
7. All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

8. Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.
9. Any change of an ITS documentation set goes through change control process
10. The defined rules on the Information Transfer policy are followed in case of sending documents and messages to the wrong number either by misdialing or using the wrong stored number.
11. Documentation sets are reviewed and updated periodically to ensure that they are up to date and current.
12. By default, security documentation is classified as a minimum of C3/RESTRICTED

7. RESPONSIBILITIES

Responsibilities towards this policy shall be clearly identified in procedure document:

1. For enforcing the policy and ensuring its implementation, in addition to the continuous review of the policy to ensure its validity over time.
2. Support and commitment towards ensuring of the implementation of this policy.
3. Ensure compliance with this policy.

PL-IS-SG-13: Audit and Certification Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

ITS is committed to improving its processes and the security of the assets with which it is entrusted. To demonstrate this commitment, the department undergoes periodic internal and external audits to show compliance with adopted policies and standards.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure that an adequate governance and security improvement program is established and managed by the IT Services Department, which follows an adopted security management system standard.

4. SCOPE

Governance frameworks or standards adopted by the IT Services Department, such as ISO 27001 (ISMS) or the Qatar National Information Assurance Policy (NIAP).

5. AUDIT AND CERTIFICATION[1]

The IT Services Department shall:

1. Ensure the establishment of a governance and security improvement program.
2. Comply with relevant provisions of State Laws and regulations that exist at the time and those, which may be amended and / or added later in time.
3. Be audited by a Certification Body or an independent body.
4. Ensure that an audit of its Information Systems (infrastructure, people and processes) is carried out at least once every year or whenever it undergoes a change that may affect the security of the University.
5. Ensure that the identified scope of the audit process includes all information assets, people and processes.
6. Ensure that recertification is carried out where any change or new finding invalidates or calls into question the current accreditation. Full certification is required for major changes affecting the basic security design of a system and a partial process is needed where the change is moderate or affects two or more security requirements.
7. Ensure that all non-conformance is fixed in a defined timeline.
8. Ensure that any exemptions are approved by the Certification Body.
9. Plan and perform internal audits of Qatar 2022 Cybersecurity Framework[2] Capabilities, and identify the scope of the Cybersecurity Capabilities Self-Assessment to be covered in the assessment / audit exercise that are applicable to the Qatar University.
10. Determine the skillset / competency required for the internal audit / self-assessment exercises carried out for Qatar 2022 Cybersecurity Framework Capabilities.
11. Formalize the internal audit/self-assessment report for in-scope cybersecurity capabilities, and ensure to evaluate and review the results with the relevant stakeholder and senior management, and ensure that it is in line with requirements of the relevant capabilities.
12. Report the final internal audit/self-assessment report on Qatar 2022 Cybersecurity Capabilities to MPT Office.

[1] Reference: Qatar National Information Assurance Policy 2.0
[2] Reference: Qatar 2022 Cybersecurity Framework 1.0

PL-IS-SC-02: Network Security Policy

Contents: • Policy Description • Who Should Know This Policy • Purpose • Policy	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses QU network management and access.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to govern the deployment and management of networks at Qatar University.

4. SCOPE

This policy applies to all Qatar University networks.

5. POLICY STATEMENTS

The IT Services Department is the central authority for all QU network services, including Local Access Network (LAN), Wide Area Network (WAN), Internet access and remote access to the internal network. To properly manage and secure network access, ITS:

1. SHALL embed security principles and tools into the design, building, and operation of networks and associated interconnections. This includes the use of VLANs, port security, network edge authentication, firewalls, application-level encryption, and network configuration management processes and tools.
2. SHALL restrict access to the local network to authorized devices, and provide facilities to encrypt network traffic using strong encryption algorithms.
3. SHALL dedicate one or more networks for device and system management and require the use of secure channels to connect to and manage systems and devices (e.g. VPN, SSH, etc.).
4. SHALL maintain documentation for all QU network connections, internal and external. Device configurations should be review.
5. SHALL provide secure channels to access to internal QU resources from remote locations, e.g. VPN.
6. SHALL follow vendor guidelines to harden network devices.
7. SHALL solely manage Internet access for QU and ensure that controls are in place to:
    a. Protect internal QU systems from external network threats
    b. Block access to sites that might contain offensive, abusive or harmful material. These websites are defined into categories that change over time
    c. Scan incoming and outgoing Internet traffic for malware and block it if necessary
    d. Facilitate logging of user activity to help in technical troubleshooting or digital forensics.
8. SHALL have the right to block or disconnect unauthorized devices from the network, including user-installed network equipment such as wireless access points, switches, etc.
9. MAY restrict or completely block access to the network in response to observed and documented risks associated with a device.
10. MAY restrict or block access to peer-to-peer networks across its network due to the high risks associated with such access.
11. MAY monitor and track users' wired or wireless devices and log their network activity to assist in incident management or digital forensics.
12. CAN grant limited third party access to QU campus network resources based on the requirements of a QU business unit, within the limits of the QU and third party agreement.

5.1 Virtual LAN Security

- Organization shall ensure to disable trunk/port mirroring on switches managing VLANs of different classification without proper compensatory controls.

5.2 Multifunction Devices (MFD)

- Organization shall ensure the MFDs connected to network shall process the information only if the information classified at the level of their network connectivity classification or below.

5.3 Domain Name Service Server (DNS Server)

- Organization shall own and locally host DNS for accessing public domain. Organization may use the Government DNS that is part of Government Network as a primary DNS.
- Organization shall digitally sign and implement cryptographic controls for mutual authentication of DNS zone files where appropriate.
- Organization shall implement security controls such as cryptographic origin authentication and integrity assurance of DNS data to ensure confidentiality and integrity of data residing on DNS server.
- Organization shall ensure to restrict DNS services such as zone transfer to authorized users and systems only.

5.4 Email Security

- Organization shall be compliant with Sender Policy Framework (SPF) [RFC4408].
- Organization shall ensure that internal email distribution list is restricted to internal usage and shall not be addressable from the entities external to the agency.

5.5 Wireless Security

ITS shall:

- implement protocols that are tested as secure. Additionally, security controls such as VPN, dynamic key exchange mechanism shall be implemented.
- regularly monitor the network for rogue or unauthorized wireless access points.
- locate access points and/or monitor them to deter or minimize network-tapping attempts.
- ensure secure client-side settings for 802.1x such as server certificate, specify the address and disable it from prompting users to trust new certificate/server.
- ensure to change the default password, username, SSID names, encryption keys, SNMP strings etc. at the time of installation.
- regularly change the encryption keys for the non-public wireless access points. SSID broadcasting should be disabled and MAC address filtering shall be implemented if applicable.
- implement firewall/router between access point and network to filter the connections. Additionally, the firewall/router shall be configured with restrictive rules to allow only needed ports.
- deploy wireless IPS/IDS to monitor the threats of network with C3+.
- deploy separate SSIDs with different configurations for different VLANs or based on business

requirements.

5.6 Clock Synchronization

ITS shall:

- ensure to secure NTP server as per the best practices recommended.
- may use Qatar Government NTP server as a primary NTP server.

5.7 Virtual Private Network (VPN)

ITS shall:

- configure VPN to disconnect automatically after a pre-defined period of inactivity and user need to logon again to reconnect to the network.
- not permit dual/split tunneling unless suitable controls are implemented and shall permit only one connection at a time.

5.8 Voice over IP (VoIP)

ITS shall:

- implement controls such as SRTP and disable unnecessary voice protocol.
- ensure to define policies and procedures and implement security controls such as VPN, regarding the use of soft phones.
- enable port security features on the network LAN switches that connect VoIP devices.

5.9 Internet Protocol version 6 (IPv6)

- Any technological change shall be assessed prior the implementation. Organization shall start considering IPv6 deployment.
- ITS shall conduct risk assessment to assess the threats and vulnerabilities in operating a dual stack environment.
- ITS shall consider recertification in case of any major technological change such as IPv6.

5.10 External Network Security

The intent of this policy is to protect organizational information assets and reputation by providing security requirements to any host connected to an external network of QU.

- System Administration Team must receive proper authorization from immediate supervisor to allow users to connect to an external network.
- Services and trust extended from external networks shall be limited to the minimum necessary to accomplish the task requiring the connection.
- Both parties (trading partners) to an external network may audit the security of the connection.
- Questionable or unusual activities shall be immediately reported to the IT Assurance Team.
- Organizational sensitive or proprietary information shall not be stored on an external network unless risks are assessed and proper approvals are obtained for such storage.

5.11 Internet Access/Firewall Security

A perimeter firewall is a gateway that limits access between networks in accordance with Organizational Internet Access/Firewall Security Policy. This system, or combination of systems, enforces a boundary between two or more networks. All traffic from the inside out and outside in must pass through it, and only authorized traffic is allowed to communicate.

ITS shall:

- divide the network shall into different sub-nets as appropriate to the requirements. The sub-nets shall be protected using appropriate firewall protection.
- provide Internet access through firewalls and security processes.
- ensure to place firewalls between organizational network and the Internet to prevent unauthorized access to organization network.
- return the failed firewalls to service by authorized personnel only.
- ensure that the firewalls always perform security checks before routing packet from one network interface to another.
- shall not accept traffic on their external interface that appears to be from internal network addresses.
- shall audit the network traffic. Both approved and unapproved connections shall be audited.
- Ensure that firewall audit logs are be stored in a secure manner, such that only authorized personnel may access them.
- ensure that the firewalls is configured to deny all inbound connections except those that have been previously approved.
- ensure that appropriate firewall documentation shall be maintained offline all times.
- ensure that firewall configurations shall be tested offline and verified before placed into service.
- ensure the Information Assurance Team evaluates new releases of patches for firewall software, before implementation.
- ensure that the new releases of patches for firewall software only be obtained from the vendor or another trusted source.
- ensure that the Information Assurance Team approves firewall configuration changes before being implemented.
- ensure details of QU internal network is not be visible from outside the firewall.
- Ensure that firewalls are run on dedicated appliances, only software or services essential to firewall operation shall be installed or run.
- Ensure that physical access to firewall is limited to members of the Information Assurance Team and others as required to ensure proper operation, e.g. Network and Telecommunications Team.
- Ensure that physical and logical access to diagnostic ports shall be given only with proper authorization. The port(s) shall be disabled after the use.

5.12 Cabling Security

ITS shall:

- maintain cables register comprised of at least the following:
    - Cable identification number
    - Classification

  - Source
  - Destination
  - Floor plan diagram
- review and update cables register on periodic basis.
- may maintain redundant communication pathways to ensure continued connectivity.
- implement controls that include educating users on the permitted level of classified conversations on both the internal and external telephone connections and level of encryption implemented.

5.13 Gateway Security

ITS shall:

- implement security controls prior to connecting internal network via gateway to external entity or public network such as:
  - devices to control all data flows/rules
  - gateway components shall be placed in physically secured server room
- classify the gateway in-line with the information it processes or transmits and the security controls and labelling shall be implemented accordingly.
- configure and manage gateway appliances rules as per the recommended industry best practices.
- implement security hardening prior to any implementation/deployment of gateway appliance in the production environment. Key security threats that shall be considered are:
  - Poor configuration
  - Information/data leakage
  - D/DoS attacks
  - Rogue network monitoring
  - Malicious code and vulnerabilities
  - Wrong or poor configurations
  - Account compromise and unauthorized or inappropriate privilege escalation
- ensure that the gateways are able to identify, drop or block content such as:
  - Offensive language or attachment
  - Categories of website/content defined as inappropriate in the Cyber Crime Law including sites hosting obscene material, gambling sites, etc.
  - Malware infected content
  - D/DoS attacks
- tie down the accountability of data export on system users for exporting data. They shall ensure to classify, label as per the classification and necessary controls are implemented accordingly.
- ensure to employ content filtering mechanism at gateways to perform keyword searches on textual data that is being exported to external entities/organizations.
- tie down the accountability of data import on system users for importing data. They shall ensure to classify, label as per the classification and necessary controls are implemented accordingly.
- Ensure Monitoring and supervision of gateways is in place and include threat prevention mechanisms, logging, and alerts.

6. EXCEPTIONS

Exceptions to this policy must be reviewed and approved by the IT Director.

PL-IS-SC-03: Information Exchange Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The exchange of confidential information between QU and other entities should be thoroughly understood and agreed to by all parties. Formal agreements are necessary to ensure compliance and to eliminate any ambiguities in understanding each party's responsibility toward securing the shared information.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☒ Office of the General Counsel
☒ Dean
☒ Director/Department Head
☒ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure that information exchange is controlled and provides for the necessary security controls. The exchanged information via electronic messaging should be protected from unauthorized access, change or interruption of service.

4. SCOPE

The exchange of confidential QU information with external parties.

5. POLICY STATEMENTS

The Information Technology Services department shall maintain compliance with ISO 27001 and the Qatar National Information Assurance Policy with regard to information exchange. To achieve this, QU shall take into consideration the following:

1. Ensure that agreements between entities exchanging information have been established prior to information exchange. Such agreements shall include details on what is being exchanged along with clauses that assure agreed-to levels of confidentiality and integrity.
2. Prior to establishing cross-domain connectivity, QU shall evaluate, understand and assess the structure, security and risks of other domains. This risk review shall be documented for compliance requirements.
3. When using communication facilities to transfer information:
    a. procedures for the detection of and protection against malware shall be defined and documented
    b. policy or guidelines outlining acceptable use of communication facilities shall be defined and documented
    c. cryptographic techniques are used when required
    d. retention and disposal guidelines for all business correspondence are maintained
4. Ensure the exchanged information via electronic messaging is protected from unauthorized access, change or interruption of service, in addition to:
    a. ensuring correct addressing and transportation of the message
    b. reliability and availability of the service
    c. legal considerations,
    d. obtaining approval prior to using external public services
5. For outgoing email, a disclaimer or similar notice should be attached, in addition to taking into consideration the classification of information. Message content that is rated C2 or above must be encrypted and properly handled.
6. Limit the information provided to the general public (via media outlets), to sanitized and approved information, through a designated and trained media relation spokesperson

PL-IS-SC-05: Product Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The complexity of IT systems and services demands that their deployment and management be controlled in order to ensure stability, security and useful life. Security compliance is usually considered late in the process of procuring IT systems or services, which can result in a suboptimal or highly risky environment where QU data may be at risk of unauthorized disclosure.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to define the importance of including security in the process of IT system acquisition and deployment.

4. SCOPE

This policy applies to planned IT system deployments at Qatar University.

5. DEFINITIONS

IT System	Any combination of hardware, software, and/or IT service(s) that will access and/or process Qatar University data.

6. POLICY STATEMENTS

The selection and acquisition of IT systems must undergo a proper selection and acquisition process that takes into consideration the associated risks.

ITS must ensure that:

1. IT system selection is carried out with due diligence and ensures product and vendor independence.
2. The selection process includes proper vendor identification and screening, using evaluation criteria which include:
    a. Vendor status and identification, including location and ownership
    b. Financial situation
    c. References from previous successful engagements
    d. The ability of the vendor to build and/or maintain appropriate controls as determined by a risk assessment
3. Proper testing and effective matching between vendor's claim and functionality is carried out, to avoid loss of confidentiality, integrity and/or availability.
4. Security requirements (functional, technical and assurance requirements) are developed and implemented as part of system requirements.
5. Products are purchased from developers that have made a commitment to the ongoing maintenance of the assurance of their product.
6. Product patching and updating processes are in place and are in line with the change management procedure.
1. All applications (acquired and/or developed) are available for production use only after appropriate quality and security assurance tests and checks to ensure that the system confirms and complies with the intended security requirements.
2. Systems comply with all legal requirements including license, copyrights, intellectual property rights, etc.
3. All systems are adequately documented.
4. Source code of custom developed critical applications is available and in the case of commercial applications (serving critical applications / processes), the University SHOULD look into options of arranging an escrow for the source code.

7. EXCEPTIONS

There are no exceptions to this policy.

8. COMPLIANCE

Failure to comply with this policy may result in delay or cancellation of the system under consideration. Repeated non-compliance incidents will be reported to QU administration for further action.

9. EXCEPTIONS

Exceptions to this policy must be submitted to the IT Director for further evaluation. Approved exceptions are then documented and communicated to the requesting party.

PL-IS-SC-06: Software Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The purpose of this policy is to ensure that appropriate information security controls are implemented for all of the QU application development activities, whether in-house or through third party contractors. The policy also covers security controls for commercial applications deployed at QU.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to assert the importance of including security in the process of software development and acquisition and not post acquisition or development.

4. SCOPE

This policy applies:

1. Software developed for use at Qatar University by internal or external parties.
2. Operating system and application software acquired by QU
3. Web applications
4. Databases

5. DEFINITIONS

SDLC	The software development life cycle (SDLC) is a framework defining tasks performed at each step in the software development process.
Escrow	A bond, deed, or other document kept in the custody of a third party, taking effect only when a specified condition has been fulfilled.

6. POLICY STATEMENTS

To keep risk to an acceptable level, the Information Security Manager shall ensure that proper security controls are implemented for each application developed. These controls may vary in accordance with the sensitivity and criticality of each application.

6.1 Software Development and Acquisition:

Software development and acquisition activities shall ensure that[1]:

1. Security is considered in all phases of the software development life cycle (SDLC) and that is an integral part of all system development or implementation project.
2. All applications (including new and developed) are classified and accorded security protection appropriate to their confidentiality, integrity, and availability ratings.
3. Security requirements (functional, technical and assurance requirements) are developed and implemented as part of system requirements.
4. Dedicated test and development infrastructure (systems and data) are available and are separate from production systems. Furthermore, information flow between the environments SHALL be strictly limited according to a defined and documented access control policy, with access granted only to system users with a clear business requirement and write access to the authoritative source for the software SHALL be disabled.
5. All applications (acquired and/or developed) are available for production use only after appropriate quality and security assurance tests and checks to ensure that the system confirms and complies with the intended security requirements.
6. Software developers use secure programming practices when writing code, including:
    a. complying with best practices,

[1] Reference: Qatar National Information Assurance Policy 2.0

   b. designing software to use the lowest privilege level needed to achieve its task
   c. denying access by default
   d. checking return values of all system calls
   e. validating all inputs
7. Software should be reviewed and/or tested for vulnerabilities before it is used in a production environment. Software SHOULD be reviewed and/or tested by an independent party and not by the developer.
8. Systems (acquired and/or developed) comply with all legal requirements including license, copyrights, IPR etc.
9. All systems (acquired and/or developed) are adequately documented.
10. Source code of custom developed critical applications is available and in the case of commercial applications (serving critical applications / processes). The University SHOULD look into options of arranging an escrow for the source code.

6.2 Software Applications

In order to comply with this policy, ITS must ensure:

1. All server and workstation security objectives and mechanisms are documented in the relevant system security plan.
2. Workstations use a hardened standard operating environment
3. Potential vulnerabilities are reduced by:
   a. Removing unnecessary file shares
   b. Ensuring patching is up to date
   c. Disabling access to all unnecessary input/output functionality
   d. Removing unused accounts
   e. Renaming default accounts
   f. Changing default passwords
4. All software applications are reviewed to determine whether they attempt to establish any external connections. If applicable, ITS should assess the risks associated with allowing or denying such connections and take appropriate action.

6.3 Web Applications

In order to comply with this policy, ITS must ensure that:

1. All active content on QU web servers is reviewed for security issues. ITS should follow the documentation provided by the Open Web Application Security Project (OWASP) guide to building secure web applications and web services.
2. Personal information and sensitive data are protected whilst in storage and in transmission using appropriate cryptographic controls.
3. Web sites that need to be authenticated use SSL certificates.
4. Web application firewalls are used for applications with medium or higher risk rating.

6.4 Databases

In order to comply with this policy, ITS must ensure that:

1. Database files are protected from access that bypasses the database's normal access controls.

2. System users who do not have sufficient privilege to view database contents cannot see associated metadata in a list of results from a search engine query.
3. Sensitive data in databases shall be masked using data masking technology for C3 (Restricted) and above classification.

7. EXCEPTIONS

Exceptions to this policy must be submitted to the IT Director for further evaluation. Approved exceptions are then documented and communicated to the requesting party.

PL-IS-SC-08: Media Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses the need to control electronic media used to store QU information.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to mitigate the risk of disclosure, modification, removal and destruction of information stored in removable media.

4. DEFINITIONS

Removable / portable media	Removable media is any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-ray disks, USB storage devices, etc.

5. SCOPE

This policy applies to the use of removable media that store QU data.

6. POLICY STATEMENTS

In order to comply with this policy, ITS must ensure that:

1. Confidential information is stored on removable media only when required to conduct business, and after applying appropriate security controls.
2. Media containing confidential information is:
    a. classified and labeled according to the highest classification level of the content.
    b. protected from theft, loss, or unauthorized access.
    c. properly sanitized or destroyed when no longer needed.
3. The loss, theft or unauthorized destruction of removable media or portable devices that contain QU Information is reported to the relevant business unit head for further assessment of the associated risks.
4. For off-site storage of media such as backup tapes, appropriate privacy and security agreements are in place with the storage service provider.
5. QU-employed couriers or contracted Third Party couriers are used to transport media or devices with a classification of confidential or internal use.
6. Media used for forensics analysis are stored in a secure environment with appropriate controls to maintain the chain of custody and integrity of original media content.
7. Media used to hold classified information may be declassified after:
    a. The information on the media has been declassified by the originator, or
    b. The media has been properly sanitized. If the storage media cannot be sanitized, then it cannot be declassified and must be destroyed when no longer needed.

6.1 Media Sanitization, Repair and Maintenance

QU shall ensure that:

1. A documented procedure exists for the sanitization of media.
2. Non-volatile magnetic media is sanitized by securely overwriting or degaussing it.
3. Appropriately vetted and briefed personnel carry out repairs and maintenance for hardware containing classified information.

4. Repairs on systems containing classified information rated C3 or above are carried out under supervision.
5. Records of media destruction and disposal activities are logged.

7. EXCEPTIONS

For media where labeling is not feasible or unwarranted, reasonable means to identify the media ownership and content may be used.

PL-IS-SC-09: Access Control Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses the fundamental requirements for user identification, authentication and authorization to access and use QU IT resources.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

This purpose of this policy is to address the deployment and use of a variety of access control solutions to ensure the confidentiality, integrity and availability of QU information assets, and to ensure secure and reliable operation of the University's information systems.

4. DEFINITIONS

Term	Definition
AD	Microsoft Active Directory, the central repository of all QU accounts.
LDAP	Lightweight Directory Access Protocol – a networking protocol used to access and use a directory services.
Account	An account that is created to access a system or resource.
Central Account	An account that is created on a central directory system such as AD or LDAP
Local Account	An account that is created on an individual system or database
Account attribute	An attribute related to the Account, e.g. creation date, status, full name, title, department or college, etc.
Username	In the context of this policy, the username is the same as the Account
External Attribute	An Attribute that originates from a system that is external to central directories, e.g. the full name of an individual

5. SCOPE

Access to QU information systems.

6. POLICY STATEMENTS[1]

The access control security policy is divided into the following control areas:

- General
- Identification and authentication
- System access
- Privileged access
- Remote access

6.1 General

The University shall ensure that:

1. Users are provided access based on the principle of "least privilege" and governed by a "need to know" or a "need to have" basis.
2. Access is managed and controlled through system access controls, identification and authentication and audit trails based on the sensitivity of the information.
3. Access rights of a user or entity to create, read, updated, delete or transmit QU information are based on a matrix (hierarchical) model of rights defined by business rules established by the owners of that information.
4. A process is established which, upon any employee role or status change (including termination), ensures that information system access is updated to reflect the employee's new role.

[1] Reference: Qatar National Information Assurance Policy 2.0

5. System users who need additional access to bypass security mechanisms for any reason seek formal authorization from the Information Security Manager.
6. Any unauthorized effort to circumvent the access control is perceived as a security incident, and is handled in accordance with established incident handling procedure and/or appropriate human resources policies and procedures.
7. Audit logs are enabled and maintained in such a manner as to allow compliance monitoring with government and QU policy and to assist in incident management.
8. Logical access to QU networks is technically controlled.
9. Secure records are maintained for the life of the system to which access is granted of:
    a. all authorized system users
    b. their user identification
    c. who provided the authorization to access the system
    d. when the authorization was granted
10. Whenever technically possible, logon banners are displayed before access to systems is granted. These banners should cover the following terms and conditions:
    a. access is only permitted to authorized system users
    b. the system user's agreement to abide by relevant security policies
    c. the system user's awareness of the possibility that system usage is being monitored
    d. the definition of acceptable use for the system
    e. legal ramifications of violating the relevant policies.
    f. Wherever possible requires a system user response, as acknowledgement
11. Centralized authentication repositories such as Active Directory (AD), LDAP, authentication databases, etc. are protected from denial of service attacks and use secure and authenticated channels for retrieval of authentication data. Such repositories shall log the following events:
    a. Unauthorized update/access
    b. Start and end date and time of activity, together with system identifier
    c. User identification (for illegal logon)
    d. Sign-on and sign-off activity (for illegal logon)
    e. Session/terminal or remote connection
12. A periodic review of user accounts and access is conducted and any identified discrepancies reported and corrected.

6.2 Identification and Authentication

The University shall ensure that:

1. A set of policies, plans and procedures are developed and maintained, covering system users' identification, authentication and authorization
2. System users are educated of the policies and procedures.
3. All system users are uniquely identifiable and authenticated on each occasion that access is granted to a system.
4. Individuals who are not students, employees, contractors, or consultants are not granted a user account or given privileges to use the University's information resources or communications systems unless explicitly approved by the Information Security Manager who SHALL check that appropriate agreements, clearance and access forms have been completed.

5. Alternate methods of determining the identification of the system user are in place when shared/non-specific accounts are used.
6. Unprotected authentication information that grants system access, or decrypts an encrypted device is located on, or with the system or device, to which the authentication information grants access to.
7. System authentication data whilst in use is not susceptible to attacks including, but not limited to, replay, man-in-the-middle and session hijacking
8. A password policy that defines parameters such as length, age and complexity is defined and enforced whenever technically possible.
9. System users cannot change their password more than once a day and the system forces the user to change an expired password on initial logon or if reset.
10. Suitable controls are set to prevent the use of weak or repeated passwords
11. Screen and/or session locks are configured to:
    a. activate after a short period of system user inactivity
    b. be activated manually by the system user, if desired
    c. lock the screen to completely conceal all information
    d. ensure the screen does not appear to be turned off while in the locked state
    e. have the system user re-authenticate to unlock the system
    f. deny system users the ability to disable the locking mechanism.
12. Access to a system is suspended after a specified number of failed logon attempts or as soon as possible after the user no longer needs access, due to changing roles or leaving the University.
13. Lost, stolen, compromised passwords are immediately reported, to the Information Security Manager who SHALL ensure the corresponding account is suspended until the password is changed after user identity verification
14. Accounts that are inactive for more than three (3) months are suspended.
15. Accounts on systems processing information rated C2, I2, A2 or above are audited for currency on at most a yearly basis.

6.3 System Access

The University shall ensure that:

1. Security policies document any access requirements, security clearances and briefings necessary for system access.
2. System users have been vetted before being granted access to a system.
3. System users have received any necessary briefings before being granted access to a system.

6.4 Privileged Access

The University shall ensure that:

1. The use of privileged accounts is documented, controlled and accountable and kept to a minimum
2. Privileged accounts are only used for administrative work
3. System administrators are assigned an individual account for undertaking their administration tasks
4. Only Qatari nationals have privileged access to systems processing information classified at C4+ unless explicit authorization for exemption to this policy is given

5. System management log is updated to record the following information:
    a. sanitization activities
    b. system startup and shutdown
    c. component or system failures
    d. maintenance activities
    e. backup and archival activities
    f. system recovery activities
    g. special or out of hours activities.

6.5 Remote Access

The University shall ensure that:

1. Remote access is not provided unless authorized explicitly by the department head and only if it is warranted by business requirements and only after due diligence has been performed to analyze associated risks and suitable controls are implemented to mitigate the identified risks.
2. Two factor authentication is used when accessing systems processing data classified at C3 or above.
3. Remote access sessions are secured by using suitable end-to-end encryption.
4. Users do not access internal systems from public computers e.g. Cyber Cafes etc. or print material to any public printer.
5. Vendor remote access is limited to situations where there are no other alternatives. In this case, initiation of the connection SHALL be controlled and monitored. Vendor remote access SHALL only be for a defined period of time, dictated by the duration of the task being undertaken.

7. EXCEPTIONS

Exceptions to this policy may include accounts that are necessary to maintain long-term services such as student email accounts.

PL-IS-SC-10: Cryptographic Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy establishes the baseline for the use of encryption technologies for keeping information assets confidential and/or integral. As a custodian of public and confidential information, the University must further protect private and sensitive data/information from all cyber threats and vulnerabilities whether external or internal to the University.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of the policy is to set forth policies related to the use of encryption technologies at Qatar University.

4. SCOPE

This policy applies to critical data rated C2 and above while in motion or at rest.

5. DEFINITIONS

Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

6. POLICY STATEMENTS

1. Qatar University shall comply with laws and regulations relating to the encryption of classified data.
2. Information assets classified as C2 and above shall be encrypted and protected against unauthorized disclosure when stored and/or in transit.
3. Appropriate protocols, as defined in the Qatar National Information Assurance policy, are used for securing data classified as C3 when in transit.
4. Passwords must always be encrypted/hashed and protected against unauthorized disclosure.
5. Privileged access authentication information shall be stored off-site along backup files to ensure complete recovery.
6. Organization shall ensure to implement protocols that are approved algorithms (see the list in NIA Policy v.2.0 Manual; Appendix B) for information that is classified as C3 or above:
    - secure file transfer: SFTP
    - secure web traffic: TLS (256+bits)
    - secure remote access SSHv2 or IPSec
    - only S/MIME v3 or better for email

6.1 Encryption Algorithms and Key Lengths

The desired effect of the encryption algorithm, combined with the length (strength) of encryption keys, is to prevent reasonable attempts of cryptanalysis if a transmission is intercepted, or if the encrypted information is retrieved from storage. The encryption standard and processes are intended to ensure the security of information throughout and beyond its useful life. It shall be assumed that all data subject to encryption can be intercepted at some point and thus must be protected with an encryption algorithm of "sufficient strength" and key length of "sufficient length."

The design and strength of all key lengths of the AES algorithm (i.e.128, 192 and 256) are sufficient to protect classified information up to the CONFIDENTIAL level.

Encryption Algorithm

The encryption algorithm used shall be an industry accepted standard. Encryption technologies that are outdated, unproven and proprietary to QU are specifically prohibited. The minimum acceptable encryption algorithms for use within QU are:

- Symmetric Key: AES-256
- Asymmetric Key: RSA with 2048-bit key

Hashing

SHA-2, SHA-3 should be implemented where required.

6.2 Deployment of Encryption Technologies

Encryption technology shall always be implemented with platform level cryptography where required.

Web-based Internet Facing Applications

TLS1.2 shall be used, only with strong SSL ciphers. This standard is driven more by the state-of-the-market than the state of technology. Anything less than these requirements are currently known to be breakable by current CPUs in a reasonably small time.

File Transmissions

All file transmissions shall be encrypted.

Storage Encryption

All information shall be encrypted when stored as required by classification and/or regulation.

Messaging Technology

Sending bank card account numbers, PII or other sensitive data unencrypted via end-user messaging technologies (e.g., email, instant messaging) shall be prohibited. The transmission of other information via messaging systems shall be encrypted as required by classification and/or regulation.

Removable/Portable Media

The ability to store information on removable or portable media (i.e., USB drives, CD/DVD, smart phones) shall be restricted. If the use is authorized, "Storage encryption" requirements specified in this section apply.

Laptops

All QU-owned laptops shall be protected using a QU-approved full disk encryption solution.

Servers/Desktops

Information on QU-owned or managed servers and desktop systems shall be encrypted using a QU-approved full disk encryption solution. Systems that are physically secured within a data center where access is restricted do not require encryption.

Wireless

Wireless networks used shall be secured according to the requirements specified in IT Operations and Communications Management Policy.

Backup Media

All information stored on backup media shall be encrypted as required by regulation.

6.3 Key Management

Key management shall be in place to support the organization's use of cryptographic techniques.

Encryption Principles and Key Management

Public Key Infrastructure (PKI)

The use of public keys, private keys, and digital signatures shall be used to provide strong authentication and nonrepudiation.

- Controls shall be implemented over the issuance and administration of digital certificates and key pairs including but not limited to:

- Security modules
- Dual-control over private keys
- Secure storage of original and backup keys
- Utilize an authorized digital certification authority to validate certificates
- Ensure digital certificates are valid before accepting transactions

Pass-phrase

If a solution requires a "pass-phrase" or an administrator password to gain access to critical private key rings or other core security information, the pass-phrase shall be robust in content and of sufficient length. Additional requirements include:

- The pass-phrase value shall be assigned by local Security leadership and shall comply with Internal Credentials requirements.
- The pass-phrase value shall be known by a minimum number of QU employees that have a specific functional support role in the solution.
- The pass-phrase value shall be changed as soon as possible following the termination or resignation of any employee with knowledge of it.

Protection

Private keys shall be securely stored and protected against both disclosure and misuse. Effective controls shall be in place limiting the accessibility of all keys to appropriate employees.

- Restrict access to encryption keys to the fewest number of custodians necessary.
- Store encryption keys securely in the fewest feasible locations and forms.
- Implement controls to monitor access to encryption keys, including monthly entitlement reviews and activity reports and reviews.

Documentation

All key-management processes and procedures, including the following list, shall be fully documented:

- Generation of strong encryption keys
- Secure encryption key distribution
- Secure encryption key storage
- Periodic encryption key changes (at least annually or as required by regulation)
- Retirement or replacement of old or suspected compromised encryption keys
- Split knowledge and establishment of dual control of encryption keys
- Prevention of unauthorized substitution of encryption keys
- Requirement for encryption key custodians to sign a form stating that they understand and accept their key custodian responsibilities

7. COMPLIANCE AND EXCEPTIONS

For any deviation from the set the policy, prior approval from Information Security Manager is required.

PL-IS-SC-11: Portable Devices and Working Off-Site Security Policy

Contents:	Version Number:	4
• Policy Description • Who Should Know This Policy • Policy • Policy Sections • Restrictions • Exceptions	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses the use of personal devices on the QU network and provides a baseline of security controls that must be implemented for high to medium risk users. This policy is sometimes referred to as the "Bring Your Own Device" or "BYOD" Policy.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☒ Faculty
☒ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

This policy puts forth some requirements that high and medium risk users must follow when connecting their personal devices to the QU network infrastructure.

4. DEFINITIONS

Term	Definition
High and Medium Risk Users	QU executives, officials and individuals who handle sensitive employee and student information
Low-risk Users	Users who do not store any QU sensitive information on their mobile devices. This can include students and office workers who use their QU-provided desktop for all their work and do not handle any sensitive information.

5. POLICY STATEMENTS

Qatar University recognizes the value of allowing its users to access internal IT resources from remote locations. QU also recognizes the risks of connecting to internal QU resources from an external location, which may or may not have proper security controls in place.

In order to balance security with convenience, the Information Technology Services (ITS) department is responsible for providing a secure and controlled method to access internal IT resources from external networks.

As such:

1. Prior to accessing QU information from remote locations, users must ensure that the device from which they access QU resources is properly protected, including the installation of the latest system patches and up to date anti-malware software.
2. Users must not use public, shared computers to access confidential QU information.
3. Users must not store their login credentials (username/passwords) on any remote computer. In general, it is recommended that users NOT allow the storage of such credentials on any system.
4. After using a computer remotely, users must log out completely before leaving the device.
5. Access to QU-owned devices is limited to the individual to whom the device is issued. Users must not allow anyone else access to their device.
6. ITS may implement security controls to ensure compliance of connecting devices with minimum security requirements prior to allowing connections to be established, e.g. the presence of updated anti-malware software on the end user device.

In addition, **high and medium-risk users** must:

7. Protect their device(s) with a password, passcode or PIN.
8. Set their device(s) to lock automatically within a short period of inactivity
9. Take measures to protect their device(s) from loss or theft.
10. Not bypass the security controls set by the device's manufacturer.
11. Not allow others to use their device(s), including family members.
12. When possible, enable remote wiping or tracking of the device(s) in case of loss or theft.
13. Ensure that all data on the device(s) is properly wiped before transferring the device to someone else.

Physical security controls for Mobile/Portable Devices

- Organization shall ensure that the user is educated/aware on the physical security and responsibility of the provided information system/mobile/portable device
- Organization shall educate the user to on safely and securely handling laptops
- Users should report lost or stolen devices to the appropriate authorities and inform the IT Services Department as soon as practicable.

- Organization shall ensure to use mobile/portable devices with approved OS with all relevant patches and updates applied as and when available.
- Organization shall provide power on password as per QU's password policy.
- Organization may add a layer of protection to the laptop such as a personal firewall product or IDS shall be installed.

Virus Protection of Mobile/Portable Devices

Organization shall:

- Periodically update the anti-malware software
- Educate users to avoid opening email attachments unless it is from a reliable source.
- Ensure the user always scans any files downloaded to information system for malware from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet).
- Ensure that users report any security incidents (such as malware infections) promptly to the IT Help desk or the Information Security Manager in order to minimize the damage and awareness to be done for the same.
- Ensure to scan files/attachments for any virus before sending them outside QU.
- Use approved encryption software on all corporate laptops, choose a long, strong encryption password/phrase and keep it secure.
- Ensure corporate laptops are provided for official use to authorized employees. Do not loan laptop or allow it to be used by others such as family and friends.

Other controls for Mobile/Portable Devices

Unauthorized software

Organization shall not allow to download, install or use unauthorized software programs. Software packages that permit the computer to be 'remote controlled' (e.g. AnyDesk) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on QU equipment unless they have been explicitly pre-authorized by management for legitimate business purposes.

Unlicensed software

Organization shall ensure regarding software licenses. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate license fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period.

Backups

Organization shall take backup or provide means for users to back up of critical data/information stored on the device.

Laws, regulations and policies

Organization shall comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example.

Guidelines When Traveling

Organization shall:

- Raise awareness among users to protect their mobile/portable devices having organizational data on it while travelling.

- ensure that the employees do not leave their devices unattended/out of sight even during a security check at an airport.

6. RESTRICTIONS

In order to protect QU information systems, the Information Technology Services department may impose one or more of the following restrictions on mobile devices:

1. Block network access for devices that are identified as being involved in “suspicious” activities on the network. In such cases, blocked devices must be cleaned or patched before asking the ITS Service Desk to unblock them.
2. Restrict access to IT systems and data.

Users are responsible for supporting and maintaining their personal computing devices. ITS is not obligated to support any hardware and/or software malfunction or failure of personal computing devices.

7. EXCEPTIONS

Exceptions to this policy can be made following a properly conducted and documented risk assessment and with written approval from the respective department head or director.

PL-IS-SC-12: Physical and Environmental Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections • Responsibilities • Exceptions	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The purpose of this policy is to ensure that University information technology resources are protected by physical security controls that mitigate the risk of tampering, damage, theft, or unauthorized physical access.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure that physical access to IT Facilities is properly controlled. This will help in reducing the risk of unauthorized access and possible damage to IT equipment or disruption of IT services.

4. DEFINITIONS

IT Facilities	IT Facilities subject to controlled access and usage, including: • Data centers • Network and telecommunication rooms • ITS internal office area • ITS offices and storage locations around campus • Other areas that can seriously impact IT operations
IT Facilities Coordinator	Individual(s) assigned the primary responsibility of managing the IT Facilities

5. SCOPE

This policy applies to:

1. IT Facilities as defined above
2. IT Services Department internal office area
3. Other offices and storage areas used by ITS where access control may be required.

6. POLICY STATEMENTS

The IT Services Department (ITS) shall ensure that appropriate security measures and controls are adopted to meet the requirements of this policy[1].

General

1. A security perimeter is defined around areas that contain either sensitive or critical information or information processing facilities.
2. Equipment, information or software are not taken off-site without prior authorization.
3. Security is applied to off-site assets considering the different risks of working outside the organization's premises.
4. Users ensure that unattended equipment has appropriate protection.
5. Organization shall implement physical access controls to prevent unauthorized access.
6. Organization shall remove the dismissed employee from the office premises immediately.
7. Vendors shall be escorted at all times to ensure security at the datacenter and ITS premises.
8. Organization shall ensure that sensitive material that is discarded shall be rendered unrecoverable. For example, paper, CD/DVD, etc. shall be shredded/burnt and tapes, USB Storage Devices, Old / Damaged Hard Disk Drives shall be discarded with precaution so that the data may not be restored in future.

[1] Adapted from the Qatar National Information Assurance Policy, v. 2.0

9. Organization shall properly uninstall and store all equipment no longer required for operations.
10. Organization shall provide pest control measures periodically (half-yearly) for entire facility.
11. Organization shall protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.
12. Organization shall ensure to physically separate the cables carrying information classified as C4 or above from cables carrying information classified at C3 or below. Cables shall be secured through physically independent conduits.

Physical Entry Control

1. IT Facilities are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
2. Physical security for offices, rooms and facilities are designed and applied.
3. Procedures for working in secure areas are designed and applied.
4. Organization shall implement appropriate physical access controls to IT Facilities
5. Organization shall ensure access to all infrastructure computing and networking devices (e.g. routers, switches, firewalls, and servers) to be restricted to only privileged employees. Separate physical control and access verification shall be provided for these devices.
6. Organization shall supervise and restrict access to controlled areas of the facility (e.g. Server rooms etc.) for maintenance personnel.
7. Organization shall ensure that access to organizational facilities by support personnel (e.g. cleaning staff, building maintenance, etc.) is supervised and controlled.
8. Organization shall deploy guards or an approved security control system at all facility entrances to ensure only authorized personnel have access.
9. Organization shall validate visitors who need to enter organizational premises prior to entry and they shall be required to sign in Visitor register and shall be provided with 'Visitor' card.
10. Organization shall ensure all visitors wear 'Visitor Card 'which is prominently visible.
11. Organization shall ensure all the visitors / maintenance personnel etc. are escorted.
12. Organization shall not allow only personal visitors inside the working area.

Equipment Security

1. Physical protection against natural disasters, malicious attack or accidents are designed and applied.
2. Equipment are sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
3. Equipment are protected from power failures and other disruptions caused by failures in supporting utilities.
4. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage.
5. Cables are inspected for inconsistencies with the cable register on a regular basis.
6. Equipment are correctly maintained to ensure its continued availability and integrity.

Public Access

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, if possible, isolated from IT Facilities to avoid unauthorized access.

Storage Media Disposal

All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Electrical Power

1. Organization shall isolate and condition power supplies use to provide electrical power to those systems.
2. Organization shall install Uninterruptible Power Supply (UPS) to support network servers and other mission critical systems.
3. Organization shall provide auxiliary power by backup generator(s) where there are frequent power cuts.
4. Organization shall periodically test and evaluate backup power systems to ensure proper operation of systems and procedures.

Fire Exposure

Computer facilities are particularly sensitive to smoke and fire damage. The risks are greater for computers because, unlike buildings and office equipment, computer loss or damage involves the loss of information as well as equipment:

1. Organization shall not store paper and other flammable materials and supplies in computer equipment rooms.
2. Organization shall make Emergency telephone numbers available to security Guards.
3. Organization shall equip smoke detectors in building particularly in sensitive areas.
4. Organization shall periodically test the smoke detection system at least once in six months.
5. Organization shall conduct fire drill / training once in year.

Air Conditioning Considerations

1. Organization shall install dedicated air conditioning system to the computer facility.
2. Organization shall ensure all air ducts in the computer facility are physically protected against unauthorized tampering.
3. Organization shall properly maintain all the air-conditioning equipment.

7. RESPONSIBILITIES

The IT Facilities Coordinator is responsible for enforcing compliance with this policy and associated procedures. The Information Security Manager ensures compliance.

8. COMPLIANCE AND EXCEPTIONS

Failure to comply with this policy may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or

consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of QU Information Resources access privileges, civil, and criminal prosecution.

PL-IS-SC-13: Virtualization Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The objective of this policy is to provide controls to secure the visualized IT infrastructure at the University.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure that adequate security measures is in place to secure the virtualization platform deployed in Qatar University Datacenter.

4. SCOPE

This policy applies to virtualization infrastructure deployed in Qatar University Datacenter covering both primary and disaster recovery site.

5. DEFINITION

Virtualization	Virtualization is the process of partitioning physical computing resource into logical elements, thus resulting in logically isolated, standalone instances, such as servers and their underlying operating systems and applications.
Hypervisor	Hypervisor is computer software, firmware, or hardware, that creates and runs virtual machines.

6. POLICY STATEMENTS

Qatar University shall ensure the following[1]:

1. Evaluation of the risks associated with the virtual technologies.
    a. in the context of relevant legal, regulatory policies and legislations.
    b. how the introduction of virtual technology will change the existing IT infrastructure and the related risk posture.
2. Hardening of the hypervisor, administrative layer, the virtual machine and related components as per the industry accepted best practices, security guidelines, and vendor recommendations.
3. Adequate physical security is in place to prevent unauthorized access to the virtual technology environment.
4. The change management process encompasses the virtual technology environment.
    a. Ensure that virtual machine profile is updated and the integrity of the virtual machine image is maintained at all times.
    b. Care should be taken to maintain and update VM's which are not in active state (dormant or no longer used).
5. Logs from the virtual technology environment are logged and monitored along with other IT infrastructure.
6. If servers with multiple security requirements/classifications are placed on the same subnet, adequate security measures are in place in protect the communications between the virtual machines.

7. COMPLIANCE AND EXCEPTIONS

There are no exceptions to this policy.

[1] Adapted from the Qatar National Information Assurance Policy 2.0

PL-IS-SC-19: Cloud Security Policy

Contents: • Policy Description • Who Should Know This Policy • Overview • Policy	Version Number:	5
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The prolific use of cloud services and potential risks and compliance concerns require Qatar University to provide proper guidance for the University community regarding the use of cloud services in a manner that does not compromise the security of QU institutional information and personal information of its constituents.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☒ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☒ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to ensure that the use of cloud-based IT services is in accordance with the business and security requirements and relevant laws and regulations.

4. DEFINITIONS

Term(s)	Definition
Cloud Computing, Cloud Services, "The Cloud"	The use of computing resources that users access through a network, most commonly the Internet
Private cloud	reserved for the use of a single organization, regardless of the location
Community Cloud	used by organizations with similar interests, concerns and requirements
Public Cloud	open for public use, typically located on a Cloud Service Provider's premises
Hybrid Cloud	a combination of two or more of the above
Infrastructure as a Service (IaaS)	CSP is responsible for physical infrastructure
Platform as a Service (PaaS)	CSP is responsible for physical infrastructure and operating system.
Software as a Service (SaaS)	CSP is responsible for all aspects except the actual data

Cloud customer responsibility
Cloud service provider responsibility

Source: PCI-DSS Virtualization Guidelines, 2011

	Type of Cloud Service		
Area of Responsibility	**IAAS**	**PAAS**	**SAAS**
Data			
Software, user applications			
Operating systems, databases			
Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks, etc.)			
Computer and network hardware (processor, memory, storage, cabling, etc.)			
Data center (physical facility)			

5. POLICY STATEMENTS

Qatar University acknowledges the benefits of utilizing cloud-based services ("cloud services") and realizes that the use of such services can increase the risks to the security of QU information assets.

1. QU has full control over confidentiality and integrity. This can include encrypting data before storage and during transit.
2. Availability is guaranteed as per the data classification
3. Compliance with applicable local laws, policies, and regulations, including the National Information Assurance Policy and the Qatar Cloud Security Policy.
4. A QU business unit that is interested in procuring a cloud service must present its business case to ITS for further assessment of:
    a. Compliance
    b. Suitability of prospective cloud service providers
    c. Availability of alternative suitable solutions
    d. Technical feasibility of the proposed solution
5. Prior to procuring cloud services, risks associated with the use of cloud services must be addressed and documented. These include issues related to:
    a. Legal trans-border requirements

b. Physical security
c. Data disposal
d. Multi-tenancy and isolation failure
e. Application disposal
f. Lack of visibility into software systems development life cycle (SDLC)
g. Lack of control of the release management process
h. Identity and access management
i. Service Oriented Architecture (SOA)-related vulnerabilities
j. Exit strategy
k. Collateral damage resulting from threats to public cloud services
l. Support for audit and forensic investigation

5.1 Establish

Organization shall:

- establish cloud security strategy.
- ensure documenting cloud security policy and procedures.
- deploy and train team members for cloud infrastructure management
- authorize the use of cloud computing services for work by the IT Manager / ISM / Designated manager.
- ensure that the IT Manager / ISM / Designated manager certifies that security, privacy and all other IT management requirements are adequately addressed by the cloud computing vendor.
- ensure that for any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the IT Manager / ISM / Designated manager.
- ensure to sign Non-disclosure agreement with the cloud service provider
- ensure that the use of such services comply with QU's existing Acceptable Use Policy/ Internet Usage Policy/BYOD Policy.
- ensure that the use of such services comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by QU.
- identify and approve what data may or may not be stored in the Cloud.
- prohibit **personal** cloud services accounts be used for the storage, manipulation or exchange of company-related communications or company-owned data.

5.2 Stripping Unnecessary Services, Apps and Credentials

Organization shall:

- disable unnecessary services and ports.
- disable/remove username and credentials.
- remove all remote support and service accounts which are not to be used, besides changing, all default passwords.
- remove all unnecessary apps.

5.3 Patching and Baselining

Organization shall apply security and functionality patches on periodic basis.

5.4 Verification

Organization shall perform vulnerability scanning for verification purposes.

6. COMPLIANCE AND EXCEPTIONS

Failure to comply with this policy may result in disciplinary action against individuals and the disruption of established cloud services if deemed inappropriate or non-compliant with local laws and regulations.

Exceptions can be granted following a risk assessment and case study by the IT Services department.

PL-IS-SC-20: Digital Forensics Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

Threats to IT infrastructure and resource are increasing, and in some cases result in formal investigations that require special handling and care. A Digital Forensics policy establishes the framework for such investigations.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The "Legal and Forensic Policy" is defined to allow proper management of incidents that involve a breach of QU information security policies or other local government laws and regulations or put in jeopardy the reputation of the University or its personnel.

4. SCOPE

The Digital Forensics Policy applies to all individuals who use or handle any Qatar University information resource. Incidents covered by the policy include, but are not limited to, the following:

1. Internet misuse/abuse
2. Electronic mail misuse/abuse
3. Unauthorized use of computing resources, including computing devices and network resources
4. Storage of pornography or adult related material and illegal content
5. Unauthorized access to hardware, software
6. Violations of the QU Employee Non-Disclosure Agreement
7. Activities that warrant further investigation by QU or government agencies

5. POLICY STATEMENTS

1. QU shall investigate all incidents related to information security breaches using proper, adopted good practices and guidelines.
2. In the course of a forensics investigation, QU shall take all measures to ensure the preservation of evidence in such a way that it can be admissible in a court of law.
3. Confidentiality of the investigation process shall be maintained throughout.
4. The Information Technology Services department is the primary party responsible for all information security-related investigations and it holds the right to investigate any actions that can impact the services offered by QU, QU's reputation or incidents that violate Acceptable Use of IT Resources policy.
5. ITS also holds the right to seize the data, assets or resources used for illegal activity.
6. ITS is responsible for sharing information about the investigation with the appropriate agencies, after proper approvals, without consent of the asset owner. Such sharing shall be done with the approval of executive management.

6. RESPONSIBILITIES

Information Technology Services	Conducts or facilitates digital forensics activities
President/Vice President Office of the General Counsel	Approval for digital forensics investigation

7. PRIVACY

The Privacy clauses defined in the Acceptable Use of IT Resources Policy apply.

PL-IS-SC-21: Acceptable Use of IT Resources

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	3.1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

8. POLICY DESCRIPTION

This policy addresses the need to inform QU IT users of restrictions on the use of QU IT resources.

9. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

10. PURPOSE

The purpose of this policy is to set and communicate the terms and conditions for acceptable use of IT resources at Qatar University.

11. DEFINITIONS

Term	Definition
Computing Device	A laptop, desktop, mobile or other device used at Qatar University to access institutional data, systems, and network.
QU-Owned Device	A computing device that is owned by Qatar University, regardless of the custodian.
QU-Managed Device	A device that is managed by the IT Services Department, regardless of ownership.
QU-Supported Device	A device that is supported by the IT Services Department, regardless of ownership.
QU IT Resources	All IT resources provided by Qatar University for its constituents, including computing devices, services, digital resources, infrastructures resources such as network and Internet access.

12. SCOPE

This policy applies to all users of QU IT resources, including employees, students, vendors, contractors, consultants.

13. POLICY STATEMENTS

Qatar University provides its users with information technology resources to support the academic, educational, administrative, public service, and research activities.

Users are responsible for adhering to the highest standards of ethical, considerate and proper use of such resources to serve these purposes, regardless of their affiliation with the University.

All users of QU IT resources are required to adhere to the policy sections below. Exceptions must be approved by the ISM.

13.1 Acceptable Use

The use of QU IT Resources should be for the purposes that are consistent with the non-profit educational mission and policies and legal requirements of the University, including license agreements and terms of service of the University, and not for commercial purposes.

Users may use only the QU IT Resources for which they have authorization and for the purpose of conducting QU business.

13.2 Prohibited Use

The use of QU IT Resources should not violate local applicable laws or applicable university policies. Regardless of the source of use or location of the user, QU IT Resources may not be used to transmit malicious, harassing or defamatory content.

Users are prohibited from use other users' accounts or attempt to capture or guess other users' passwords or credentials.

Users are also prohibited from providing unauthorized users access to QU IT Resources.

13.3 Accountability

Users of QU IT Resources are individually responsible and accountable for the appropriate use of the resources assigned to them or which they are authorized to access.

13.4 Use of Computing Devices

Users of QU-owned and QU-managed devices acknowledge and accept the following:

1. QU-owned devices are the property of the University. Users should handle them responsibly and with care to avoid breaking, failure and physical damage.
2. The IT Services Department (ITS) maintains control over the configuration of their device(s) and is the final authority on what can be installed on these devices.
3. Users should not expect to have administrative privileges on QU-owned or QU-managed devices.
4. Users should not attempt to format or repair a University-managed computing device;

Users shall not use their computing devices to:

5. access illegally or without authorization: data, computers, accounts, or networks;
6. distribute offensive, abusive and/or harmful material;
7. knowingly install or distribute computer malware or other malicious software that could potentially harm systems, cause loss of data, or disrupt network services;
8. attempt to circumvent any established security measures to gain access to confidential and restricted information;
9. install or copy unlicensed software;
10. create, transmit or participate in pranks, hacking schemes, chain letters, false or deceptive information, or any other fraudulent or unlawful purposes;
11. violate local or international laws and regulations or other contractual obligations.

13.5 Use of Imaging Devices (Printers, Scanners, Copiers)

12. Printing, scanning, and copying devices and materials provided by QU are the sole property of QU and should be used for University business only.
13. Users should consider the surroundings when printing or copying confidential information, and should promptly remove the printed material from the printer.
14. Users shall not:
    a. attempt to move or remove printers and scanners from their locations without prior consent of ITS;
    b. attempt to fix a printer or scanner without contacting the ITS Service Desk for support;
    c. print or distribute abusive, offensive or unethical material.

13.6 Use of Electronic Mail

Users of QU-provided email accounts acknowledge and accept the following terms:

15. The use of electronic mail is a privilege extended by QU to its students, faculty, staff and others in order to facilitate communication in the course of conducting University business.
16. The University owns the content of electronic mailboxes of its faculty and staff and all others mailboxes created to facilitate University business, e.g. consultants and contractors.
17. The Information Technology Services Department (ITS) is responsible for managing and supporting the University's email services.

18. ITS may provide access to, or copies of the content of, mailboxes as required by QU business and/or in the course of a security forensic investigation.
19. Email accounts may be disabled:
    a. when an employee's association with the University ends. Exceptions may be granted for a specified period of time if such access is required to fulfill a business need.
    b. if they are linked to security incidents such as SPAM or other inappropriate use of email.
20. QU employees:
    a. Shall restrict the use of their QU mailbox to QU-related communication.
    b. Shall not use their QU email address for any personal activities such as registering on online sites.
    c. Shall not forward their QU mail to non-QU systems such as cloud-based email services.
    d. Shall not make offline copies of their mailboxes which may expose them to unauthorized disclosure.
    e. Do not have the right to take copies of their email when their association with the University ends.
21. All Email Users:
    a. Shall not share passwords, credit card information, and other restricted data through email without proper protection such as encryption.
    b. Shall not transmit offensive, abusive, violent, threatening and harmful content through email.
    c. Shall not transmit, forward, or post internal emails or attach classified documents containing confidential information to anyone outside of QU.
    d. Shall not transmit, forward, or post chain letter emails to anyone at any time.
    e. Shall not falsify or impersonate a sender address.
    f. Shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of QU or any unit of the QU, while communicating with domains outside QU.
    g. Shall take proper precautions to avoid falling victims for phishing.
    h. Shall not circumvent existing controls for email access.
    i. Shall report any observed irregularities to ITS for further investigation.
    j. May not use mail broadcasting for personal, commercial, and non University-related communication.
    k. Should avoid sending mass emails to users unless content is relevant to all the recipients of the mailing list.

13.7 Use of Network and Internet Access

Users accessing the Internet through QU are expected to use their access responsibly and ethically.

22. Users shall not compromise the University resources by knowingly downloading malicious, offensive, abusive, profane, illegal and/or harmful content.
23. Users should refrain from using peer-to-peer file sharing protocols due to the inherent risks associated with such use. Exceptions can be granted following proper assessment and authorization by the Information Security Manager.
24. Users shall not install or configure any active or passive network component without the express consent of ITS. This includes, but is not limited to:

a. Network access equipment (wired or wireless)
b. Network servers (e.g. DHCP, DNS, etc.)
c. Any device that consumes a disproportionate amount of network bandwidth.
d. Any device that can bypass the security mechanisms enforced by the University.

25. Users shall not bypass the security mechanism implemented and managed by QU for accessing the Internet.
26. Users shall not install devices or software that allow them direct access to their devices or systems without going through the existing security controls such as firewalls or VPN devices. Methods such as modems attached to devices or remote access software such as PCAnywhere can pose a great risk to the QU infrastructure and inadvertently allow perpetrators direct access to internal QU resources.
27. Users are solely responsible for any indirect, consequential, special or punitive damages or losses that may arise from their inappropriate use of the Internet access.

13.8 Use of Social Media

QU users of social media sites shall NOT:

28. Share QU information through social media platforms.
29. Use their personal accounts to communicate work-related information.
30. Post pictures or information that link them to QU
31. Excessively use social media in the workplace
32. Shall not represent explicitly or implicitly the University on any social media platform.

13.9 Use of Cloud Services

A risk assessment is necessary prior to the use of public cloud-based IT services to conduct QU business. The IT Services Department can assist in conducting such assessments and will provide the appropriate guidance after considering compliance, security and operational risks.

13.10 Use of Central File Storage (File Shares)

Users of the shared file storage services must comply with the following:

Departmental Shares

33. Departments are responsible for the access authorization and content of their assigned shared folders.
34. Departmental shares must undergo periodic reviews to ensure that the content is valid and that access control is properly set. The IT Services department can assist in such tasks but cannot be held responsible for any unexpected findings.
35. Departmental shares should not be used to back up individual user documents.
36. Access to departmental shares is restricted to devices managed by QU, i.e. personal computers may not be used to access such shares.

Individual Shares

37. Users of individual shares must not store any illegal or inappropriate content.
38. To ensure the security of the content stored in individual shares should back up their content to off-line storage devices. The IT Services department cannot guarantee that such content is backed up to central backup facilities.

13.11 Use of QU Web Services

39. Users and web site owners are accountable for any content that they post on QU web servers and that is deemed inappropriate by Qatar University.
40. Data classified as Internal, Limited Access, or Restricted shall not be made available via QU web sites or portal without adequate security controls.

13.12 Use of Audiovisual and Classroom Technology

ITS deploys and manages various audiovisual (AV) and classroom technology (CT) devices and services. These resources are the sole property of QU and should be handled properly and responsibly.

1. AV/CT resources may only be used in the course of conducting QU business.
2. Users may not attempt to fix any failure of the AV/CT equipment. Instead, they should report such failures to the ITS Service Desk.
3. Users may not at any time try to dismantle and/or move any AV/CT tools without prior authorization from the IT Services Department.

13.13 Use of QU ID Card

QU ID cardholders agree to the following terms and conditions ("Card" refers to the QU ID card):

41. The Card is the property of Qatar University and is non-transferable. A cardholder may allow another person to use the card in case of disability, under the direction and supervision of the cardholder.
42. Possession of the Card by any person other than the owner is a violation of University regulations and can result disciplinary action.
43. Cardholders are required to surrender their Card when it expires, is replaced, or when their association with the University ends.
44. Cardholders must present their Card should be presented upon request by security officers and University administrators, to access campus facilities, to attend events and activities, or to obtain certain services.
45. Depending on the card issuing guidelines, a Card replacement fee applies for cards that are lost or damaged due to neglect or misuse.
46. The University is not responsible for any losses or expenses resulting from the misplacement, theft or misuse of the Card.
47. Cardholders must maintain the Card in its original form with all information clearly visible (i.e. no stickers, punched holes, etc.)
48. Cardholders cannot use the Card as collateral or security for any reason.
49. Cardholders must immediately report a lost or stolen Card to the QU Security Office.
50. If found, lost cards must be returned to the QU Security Office.

13.14 Clear Screen and Clear Desk

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day or when they expected to be away for an extended period.

In order to guard the privacy of such information, employees shall ensure that:

51. Computer workstations are locked when left unattended, e.g. using a screensaver that automatically turns on after a period of inactivity.
52. Restricted and limited access information remains protected while entertaining visitors at their desk.
53. Passwords are not written down and left unprotected.
54. Portable storage devices are protected and, when no longer needed, are properly destroyed.
55. Any restricted or sensitive information is removed from open access and locked away.
56. Keys used to access safeguarded documents are not left unattended.
57. Printed material is not left unattended around printers and fax machines.
58. The secure disposition of paper documents that contain non-public information and are no longer needed. Such documents should be shredded instead of being simply thrown away.

13.15 Expectation of Privacy

While Qatar University does not generally monitor or limit the content of information transmitted on its network, it reserves the right to access and review such information under certain conditions. These include:

1. Responding to legal or regulatory requirements
2. Providing information required in the course of legal investigations
3. Investigating security incidents
4. Granting access to an employee's email and files that may be required for conducting QU business (e.g. email content of employees who no longer work at the University).

In some of these cases, the University may NOT notify the end users of the disclosure of their information.

13.16 Compliance

Users of QU IT Resources must:

1. Abide by all local and applicable laws, regulations and policies such as the Qatar Cybercrimes Law (Law 14 of 2014).
2. Abide by all copyright laws and licenses related to all forms of digital resources such as software, multimedia resources and licenses digital content.
3. Not use, copy, or distributed copyrighted works including, but not limited to, web page graphics, multimedia files, trademarks, software or logos unless they have a legal right to such use, copy or distribution.

Failure to comply with this policy may result in disciplinary action as per the QU policies and procedures.

59. Termination of access to resources provided by Qatar University, including access to wired and wireless network infrastructure;
60. Disciplinary and/or legal action as per QU policies and procedures and relevant local laws and regulations.

PL-IS-SC-22: Asset Management Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

QU has a commitment to ensure that Information Assets are managed in accordance with all relevant regulations and guidance. This policy supports the implementation, identification and management for all information assets.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

QU has a commitment to ensure that Information Assets are managed in accordance with all relevant regulations and guidance. This policy supports the implementation, identification and management for all information assets.

4. SCOPE

The policy applies to all organizational employees of QU, contractors, vendors, and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the ISM / designated representatives.

5. POLICY STATEMENTS

1. All staff shall have the necessary and suitable equipment to perform their duties and to ensure that copyright and licensing regulations are observed.
2. All staff are responsible for the assets issued to them. Ownership of Assets remains with the organization. Assets shall be safeguarded against theft and damage and removed from the premises only with approval.
3. Organization shall:
    a. ensure to operate and maintain equipment according to manufacturer's specifications.
    b. plan the asset acquisition, maintenance and replacement of information technology through asset retention / lifecycle period and Change control process.
    c. maintain information of all the vendors who all are responsible to support the assets.
    d. tag and label all the information assets with unique identity and standard.
    e. ensure that Organization shall maintain asset movement register to track the in and out of the asset from the premises.
    f. ensure to protect media containing information against unauthorized access, misuse or corruption during transportation.
    g. document any changes to an information asset in the Information Asset Register and follow the correct change control process.
    h. ensure to implement necessary procedures and controls to ensure the confidentiality, integrity and availability of the information assets.
    i. maintain an asset/risk register that is aligned with Business continuity plan based on the desired value of information assets.
    j. conduct information asset awareness throughout QU by organizing training, awareness campaigns and providing written procedures/guidance that are widely disseminated and available to staff.
    k. have in place an approved Business Continuity Plan for all critical Information Assets and all staff are aware of their roles and responsibilities.

5.1 Media Security

Organization shall:

- classify non-volatile media as per the information stored on it.

- consider re-classification of media if the:
  - information copy to the media is of higher classification
  - information stored on media is subject to classification upgrade"
- declassify the media if the:
  - information stored on the media is declassified by the data owner
  - media has been sanitized as per the organization sanitization process"

Organization shall

- sanitize volatile media by removing power for at least 10 minutes or overwriting media with random patterns followed by read back for verification
- overwrite the flash memory with random patterns followed by read back for verification.

Note: Prior to sanitization, the ITS Personnel (or the authorized person) need to take necessary backup of critical/sensitive data and make sure there is no residual data / information left over in the asset.

PL-IS-SC-23: Endpoint Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy • Policy Sections	Version Number:	4
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

Endpoint security aims to adequately secure every endpoint connecting to a network to block access attempts and other risky activity at these points of entry. Any device, such as a smartphone, tablet, or laptop, provides an entry point for threats.

This Policy is a step in this direction. It aims to help understand the roles and responsibilities of various QU functions in the context of endpoint security management.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

QU has a commitment to ensure that endpoint devices are managed in accordance with all relevant regulations and guidance. This policy supports the implementation, identification and management for all endpoint devices to build a sustainable environment.

4. SCOPE

The policy applies to all organizational endpoints such as servers, desktops, laptops, wireless devices, mobile devices, and other OT/IoT devices connected to the corporate network. Exceptions to this policy must be approved by the ISM / designated representatives

5. POLICY STATEMENTS

Organization shall:

1. identify and communicate security risks associated to the critical endpoint devices.
2. identify critical endpoints that need to be protected
3. management the endpoints connected to the corporate network.
4. enable appropriate log and event collection and analysis on critical endpoint devices.
5. identify information protection regulations and industrial compliance requirements for the associated critical endpoints.
6. implement a process where all changes to the endpoints are reported to the relevant Operations team.
7. ensure to collect and send all the endpoint security tooling logs to centralized server for analysis and monitoring.
8. implement and enforce endpoint security configurations by applying it on operating system, application and network layer.
9. ensure the application whitelisting is applied on endpoints.
10. ensure to manage reuse or final disposition of expired, obsolete devices, and unwanted endpoints in a secure manner.
11. ensure the information stored on obsolete, expired, and unwanted endpoints storage/media are appropriately sanitized.
12. maintain secure images or templates for all systems based on entities approved configuration standards.
13. deploy system configuration tool that automatically enforce and redeploy configurations on periodic basis.
14. deploy system configuration monitoring tool that verifies security configurations, catalog approved exceptions and alert when unauthorized changes occur.
15. perform vulnerability scanning of critical endpoints on periodic basis and vulnerabilities are remediated in a timely manner.
16. use automated tool to inventory administrative accounts, including domain and local account, and to ensure only authorized individuals have elevated privileges.
17. ensure to secure virtual environment such as disable unnecessary functions, isolate virtual endpoint networks and strictly control privileged account.
18. ensure the administrative accounts use MFA, and encrypted channels.
19. ensure to block access to known malicious domains and unauthorized traffic.

20. ensure to keep updated anti-malware software-- its scanning engine and database—on a periodic basis.
21. apply host-based firewall or port filtering tool on endpoint devices with a default-deny rule.
22. scan all the devices that remotely logging to the corporate network prior to accessing the network.
23. ensure that the endpoint devices have the capability to receive an automated threat intelligence from the Security Monitoring and Operations team.

PL-IS-SC-24: Clean Desk and Clear Screen Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses protecting information from being unintentionally exposed to unauthorized viewers.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

This Clear Screen Policy directs all users of screens / terminals to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. The Clear Desk Policy directs all personnel to clear their desks at the end of each working day and/ or whenever the user is away from his desk, and file everything appropriately. The purpose is to ensure that sensitive papers and documents are not exposed to unauthorized persons.

4. SCOPE

The Policy applies to all organizational employees of QU, contractors, vendors, and entities identifying threats to information assets or information systems. Exceptions to this policy must be approved by the ISM / designated representatives.

5. POLICY STATEMENTS

Organization shall:

1. lock away confidential, sensitive or critical business information, on paper or on electronic storage media, when not required, especially when the office is vacated.
2. educate users to log off / lock their machines when they are not at their desk.
3. ensure that the users have password protected screen savers activated after five minutes or screen locking mechanism. < screen savers can be ISMS awareness >
4. ensure all the users periodically clean their drawers and make sure the unwanted papers are shredded.
5. ensure that the users maintain clean desk and sensitive information is not left on the desk when they leave the desk. Such information shall also be protected from eavesdropping.
6. ensure to clear printers immediately post printing sensitive or classified information.

PL-IS-SC-25: Email Security Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses security of electronic mail at Qatar University.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

Organizational E-mail Security Policy specifies mechanisms for the protection of information sent or retrieved through e-mail. In addition, the policy guides representatives of QU in the acceptable use of e-mail. For this policy, email is described as any computer-based messaging, including notes, memos, letters, and data files that may be sent as attachment.

4. SCOPE

The E-mail Security Policy applies to all organizational employees, contractors, vendors, and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the ISM.

5. POLICY

1. E-mail Access:
    - All e-mail on organizational information systems, including company provided emails to users either in customs domain or other domains, is the property of QU.
    - The email ID is provided to the staff members to assist in carrying out the business activities and is the official ID. The Top Management can review the emails sent out from these IDs.
    - No user is authorized to access or read the e-mail of another user.
    - E-mail is provided to the users and contractors of organization to enhance their ability to conduct organizational business.
    - The size of e-mail attachment shall be limited to what is necessary for a user to perform his or her function.
    - Group ID's or Distribution List (DL) are enabled only to meet Specific requirements of Organization or particular Department. Only authorized personnel are allowed to use and Access control mechanism enabled for controlling the access.
    - Email and credentials should be shared with the Security Team if the user created an email from external domain for business purpose.
2. E-mail Content:
    - Use of, inappropriate language or misleading content in e-mail is prohibited.
    - Use of e-mail to spam (e.g. global send, mail barrage) is prohibited. This includes the forwarding of chain letters.
    - Use of e-mail for harassment is prohibited. The mail from any user should not contain any words or phrases that may be construed as unprofessional or derogatory based on race, color, sex, age, disability, national origin, or any other category.
    - Forging of email content (e.g., identification, addresses, etc.) is prohibited.
3. E-mail Usage:
    - Any e-mail activity that is in violation of the policy statements or that constitutes suspicious or threatening internal or external activity shall be reported.
    - When a user receives e-mail error messages that appear to be abnormal, they shall be reported to the System Administration Team.

- When sending e-mail, users should verify all recipients to whom they are sending e-mail messages.
- Users should understand that e-mail could be altered during transmission from the sender to the receiver, and the identities of the sender or receiver could be falsified. Users should apply common sense when assessing whether email is legitimate.
- Emails should be used strictly for the business purpose.

PL-IS-SC-26: Remote Access Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses accessing internal QU computing resources from locations that are external to the University.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

Mobile Computing, Teleworking, and Remote Access policies shall be put in place to ensure information security when using mobile computing and teleworking facilities.

4. SCOPE

The Policy applies to all organizational employees of ITS, contractors, vendors, and any other person using or accessing Organizational information or information systems. Exceptions to this policy must be approved by the ISM / designated representatives

5. POLICY STATEMENTS

5.1 Allowed Technologies for Remote Access Capabilities

- Organization shall use the below allowed remote access technologies
    - IPSEC client-based VPN (allowed only for ITS devices)
    - True SSL VPN that checks for malware and antivirus on the source machine
- Organization shall Implement Technology Requirements for Remote Access
    - Multi-factor authentication
    - Remote access configurations and VPN must not circumvent monitoring and security controls on the network such DLP, content filtering, etc.
    - Split tunneling is not allowed when connected to ITS network unless required for business operations
    - Remote access connections must have an inactivity timeout
    - VPN sessions must be re-authenticated periodically
    - Multiple VPN sessions are not permitted
- Organization shall ensure the System Requirements
    - Only corporate-approved security products and services must be used to connect and authenticate to ITS networks.
    - ODBC connections should be disabled over remote links.

PL-IS-SC-27: Password Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

The purpose of this policy is to ensure that access University information technology resources is protected by strong password security controls that mitigate the risks of unauthorized access.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☒ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

ITS recognizes that passwords are an important aspect of information security. Poorly selected, reusable password represents one of the most vulnerable aspects of information security. Organizational authorized users must comply policies to minimize risk to organization information assets.

4. SCOPE

The Policy applies to all organizational employees, contractors, vendors, and any other person using or accessing Organizational Information or Information Systems. Exceptions to this policy must be approved by the ISM.

5. POLICY STATEMENTS

1. Organization shall assign all system accounts a unique user ID and password that are protected. All initial system user accounts shall be set up by ITS as per official University records (HRMS and Student Information Systems). Other requests are documented and handled with security controls in mind.
2. Organization shall ensure that users are required to change their password after the first login.
3. Organization shall prohibit the sharing of individual passwords unless there is a business requirement and should be approved by ISM.
4. Users shall report any suspicious queries regarding passwords to the ITS Help Desk.
5. Organization shall configure that the accounts be locked out after 5 failed attempt(s). Account can be unlocked by contacting the ITS Help Desk or through a self-service portal.
6. Organization shall protect passwords as organizational proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.
7. Organization shall prohibit using programs or scripts that include system passwords unless technically required. In such cases, mitigating controls must be in place to further protect access to such passwords.
8. Organization shall enforce the users to change their passwords on a regular basis.
9. Organization shall allow the user to reuse passwords only after multiple different passwords have been used.
10. Organization shall enforce the password change for certain security events that have the potential for security compromises (i.e. employee relocation, intrusion attempt, or employee termination).
11. Organization shall allow the password change as soon as a security compromise has been identified.
12. Organization shall notify users of upcoming password expiration ahead of time.
13. Organization shall ensure that the password policy parameters meet or exceed the following:
    - Minimum of 8 character(s).
    - At least 1 special character

- At least one number (0 to 9)
- At least one capital letter (A to Z)
- At least one small letter (a to z)

PL-IS-SC-28: Capacity Management Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy is to ensure that the IT operational environment is well maintained to achieve stability of day-to-day processes and activities.

All IT equipment must be monitored regularly and a uniform process for performance and capacity management must be established. Equipment used to run key applications should be monitored more regularly.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this document is to detail the correct performance and capacity management procedure that is to be followed for systems and applications utilized in ITS.

4. SCOPE

The Capacity Management Policy applies to all employees, contractors, vendors of the organization and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the ISM / designated representatives.

5. POLICY STATEMENTS

5.1 IT Operations Management

- Organization shall design and maintain a stable IT infrastructure.
- The following areas must be managed at a minimum:
    - Server environments
    - Networks
    - Storage and archiving
    - Databases
    - Desktops / Laptops
    - Backups
    - ISP Bandwidth

5.2 Server Environment

Organization shall document server equipment and the following information must be maintained at a minimum:

- Host contact information and location of server equipment
- Server hardware and operating system version and serial numbers
- Purpose/function of server equipment and applications
- Password groups for privileged passwords
- Configuration information (server name, IP Address, and application specific information)

5.3 IT Performance and Capacity Management

- Organization shall ensure that the controlled processes are in place in the server environment and that equipment remains current, with the appropriate patches/hot-fixes. All services and applications that are unused or not serving business requirements shall be disabled except where approved by ITS.
- Organization shall conduct remote system administration (through privileged access) using approved VPN secure solutions in accordance with the Remote Access Policy.
- All system, application and security related events on server equipment shall be logged with log files archived regularly. Archival of server event logs shall meet the following minimum (or better where compliance with specific legislation is required) practice:

- All server event logs must be kept online for minimum of one week;
- Daily backups of event logs must be retained for at least one month;
- Weekly backups of event logs must be retained for at least one month; and
- Monthly backups of event logs must be retained for a minimum 3 months.
- The Administrator must complete the Daily Operations Tasks Checklist

5.4 Monthly Performance and Capacity Management Checklist

- Organization shall retain evidence of the completed and approved checklist(s).
- Organization shall define that the configuration of server equipment outsourced, or hosted by external/third-party service providers is in the contract with the service provider. At a minimum the definition must document:
  - Host contact information and location of server equipment;
  - Server hardware and operating system/version;
  - Purpose/function of server equipment and applications;
  - Configuration change management processes;
  - Backup requirements;
  - Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO); and
  - Escalation procedures.
- Organization shall isolate or otherwise disable any server equipment that has been compromised by an attacker or, otherwise places ITS' systems, data, users, and clients at risk as stipulated in ITS' IT Security Policy.
- Organization shall ensure that servers are named in accordance with the server and device naming conventions to ensure consistency.

5.5 Monitoring the IT Infrastructure

- Organization shall maintain logging of infrastructure and due care shall be taken in the protection, handling, and storage of all monitored data and logs.
- Organization shall ensure that logs record the following information on all business critical resources if the business requirements determine them to be relevant.
  - User IDs;
  - Dates/times and key events; and
  - Workstation identification and location.
- Organization shall ensure that monitoring for the use of privileged operations occurs during the following instances:
  - Systems are started or stopped;
  - Input or output devices are attached or detached; and
  - Changes and attempts to change security setting and controls.
- Organization shall ensure that monitoring for system alerts and failures capture the following details:
  - Alerts or messages from consoles;
  - Exceptions in system logs;
  - Alarms generated by network management devices or access control systems; and
  - Logs required by the Company.

- Organization shall ensure that monitoring for system access captures the following details:
    - The ID of the user;
    - The date / time of key events;
    - The type of event;
    - The files accessed and their type; and
    - The programs or utilities used during access.
- Organization shall define and implement rules that identify and record threshold breaches and event conditions. A balance must be found between logging minor events and significant events so event logs are not logging unnecessary information, thus impacting data storage capacity.
- Organization shall monitor relevant IT infrastructure capacity planning elements such as:
    - Server CPU utilization - Check if CPUs are running at full capacity or are they being under-utilized. By monitoring server CPU utilization, you can monitor server Performance and restart a process or application to improve response time for the application;
    - Server Disk utilization - Monitor the hard disk space utilized by the system and ensure critical processes on the server have sufficient system resources;
    - Server Process utilization - Monitor memory and CPU utilization of processes. This helps identify system processes or server applications using high Server Resources;
    - Network Availability – to identify data bottlenecks or specific devices on the network using more resources than expected;
    - Network traffic and Bandwidth usage - Monitor Network Interface traffic on the server and understand how much network load is being handled; and
    - Network devices (routers, switches etc.) – Ensuring that network devices are functioning as required.
    - Event logs and key indicators for critical systems and applications must be monitored and signed-off by the Administrator using the Daily Operations Task
    - Incidents must be logged, as per the Helpdesk and Incident Management Policy, in a timely manner when monitoring activities result in the identification of deviations and/or violations.
    - Infrastructure monitoring reporting must be provided by the Service Providers on a monthly basis to provide feedback. Areas that must be covered are:
    - Call logging statistics and statuses;
    - Reports on the LAN and WAN infrastructure (Routers, switches, WAN interfaces etc.);
    - Backup logs and reports; and
    - Incidents that occurred in any of the above areas.

PL-IS-SC-29: System Acquisition, Development and Maintenance Policy

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

IT systems (applications, databases and middleware) are prone to exploits due to their inherent vulnerability and misconfigurations. Security controls must be built-in through the whole system acquisition development lifecycle to ensure security requirement are factored proactively.

In addition to this and other controls, a multi-level approach to information security must be adopted at each stage of the system acquisition, system development and system deployment so that security risks are mitigated at Qatar University.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☒ Information Technology Services
☐ Procurement Department

☐ Faculty
☐ Staff
☐ Student
☒ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to define the importance of including security in the process of software development and acquisition, rather than adding it as an add-on. This policy defines security as it applies to the various phases of the Software / System Development Life Cycle (SDLC). This policy also covers security controls for commercial applications deployed within an organization.

4. SCOPE

The Policy applies to all organizational employees, contractors, vendors, and entities identifying threats to information assets or information systems. Exceptions to this policy must be approved by the ISM.

5. POLICY STATEMENTS

1. The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
2. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
3. Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
4. When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
5. Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
6. Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
7. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
8. Test data shall be selected carefully, protected and controlled.
9. Organization shall adapt security development and implementation requirements i.e. functional, technical and assurance, as a part of system requirements.
10. Organization shall ensure that all applications are tested for appropriate quality and security assurance prior to production environment. Applications shall be complied with intended security requirements.
11. Organization shall be reviewed and tested for vulnerability prior to production environment. Application shall be reviewed and tested by third party and not by the developer.
12. Organization shall document all the acquired and/or developed applications.
13. Organization shall review and determine whether the application attempts to establish any external connections or not. Organization shall make a business decision whether to permit or deny automated outbound connection functionality including the assessment of the risks involved.
14. Organization shall harden the underlying operating system and infrastructure.
15. Organization shall place a software escrow agreement with third-party vendors or applications developers where applicable and required.

5.1 Application Development

- Organization shall adapt secure coding practices such as OWASP during the application development lifecycle.
- Organization shall adapt threat modeling approach for analyzing security of an application and to address security threat associated with an application.
- Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
- Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
- The organization shall supervise and monitor the activities of outsourced system development.
- Testing of security functionality shall be carried out during development.
- Organization shall conduct design review and consider the following elements:
    - Input Validation
    - Authentication
    - Authorization
    - Configuration management
    - Sensitive data
    - Session management
    - Cryptography
    - Parameter manipulation
    - Exception management
    - Auditing and logging
    - Database security
    - Deployment and infrastructure considerations

5.2 Web application security

- Organization shall ensure to minimize/"Need to have" the connectivity and access between the web application components.
- Organization shall ensure to protect sensitive and personal information during the rest and transit via appropriate security controls.
- Organization shall ensure to implement web application firewall (WAF) for the applications having medium or higher security risks.

5.3 Product Security

Organization shall:

- Organization shall ensure that the process for procurement of IT services, solutions is fair and independent of product and/or vendor influences.
- Organization shall classify and label products as per the National Data Classification policy.
- Organization shall include proper vendor selection, screening and evaluation criteria such as:
    - financial situation

  - vendor status and identification
  - previous engagement references
  - list of risk controls maintained by vendors

- Organization shall ensure that the product delivery processes and procedures are as per the information security policies and procedures.
- Organization shall ensure secure delivery that includes measures to detect tampering or masquerading.
- Organization shall ensure that product patching and updating process implemented as per organization security policy.

PL-IS-SC-30: Operations Technology (OT) Security Monitoring

(NOTE: This draft policy is owned by the Facilities and General Services department. ITS Shared it with FGS Director on Feb 26, 2023.)

Contents: • Policy Description • Who Should Know This Policy • Policy	Version Number:	1
	Effective Date:	
	Approved by EMC on:	
	Approved by the President on:	

1. POLICY DESCRIPTION

This policy addresses monitoring of the Operational Technology environment.

2. WHO SHOULD KNOW THIS POLICY

☐ President
☐ Vice President
☐ Office of the General Counsel
☐ Dean
☐ Director/Department Head
☐ Human Resources Department
☐ Information Technology Services
☐ Procurement Department
☒ Facilities and General Services Department

☐ Faculty
☐ Staff
☐ Student
☐ Third Party Users of QU Information Resources
☐ All Users of QU Information Technology/Security Resources and Services

3. PURPOSE

The purpose of this policy is to devise a log and monitoring mechanism for organizational Operations Technology (OT) devices to detect unauthorized access, modifications and disclosure of confidential information reside on them.

4. SCOPE

This policy is applicable for all critical Operations Technology (OT) assets within QU.

5. POLICY STATEMENTS

1. Organization shall identify critical OT assets.
2. Organization shall identify critical OT logs and security audit logs for collection and analysis.
3. Organization shall define and document baseline Configuration of OT environment.
4. Organization shall implement 3-tier OT layered architecture or identify layers between existing architecture.
5. Organization shall establish change management procedure to ensure correlation of alerts with approved changes and the OT security monitoring team shall be notified upon any scheduled changes and maintenance activities.
6. Organization shall identify if any of the monitored OT asset requires mandatory safety requirement (SIL) that should be maintained all the times.
7. OT security monitoring team shall receive inputs from other teams such as SOC, Risk management that can improve monitoring such as IOCs, Threat Intelligence etc.
8. Organization shall determine OT log retention period that is minimum of 90 days as per the National ICS Security standard or legal/regulatory requirements or business requirements.
9. Organization shall subscribe to and collect threat feeds from public and community resources.
10. Organization shall ensure that any alarms, red flags and exceptions observed in the system monitoring system are registered and action is taken as per the Incident Management Process.
11. Organization shall investigate alerts and conduct appropriate triage if required.
12. Organization shall establish escalation and communication matrix to ensure relevant stakeholders are informed in the event of any breach/security incident.
13. Organization shall ensure to deploy and train team members on deployed OT technologies.