MS-IS-SG-003

ITS Information Security Policies

ISO 27001:2013 ISMS

July 2021

Produced by:	Information Technology Services Department, Qatar University
Approved by:	

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	Ebtesam Abdulla Marzouqi
Title	Manager, IT GRC Senior Risk &Compliance Specialist	Section Head of Information Assurance	Acting Director, ITS
Signature			
Date	19-05-2019	03-07-2019	03-07-2019

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

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	ITS Management	Uncontrolled
3	Qatar University Leadership	Uncontrolled
4	Information Technology Users at Qatar University	Uncontrolled

1. OBJECTIVES

This document includes all information security-related policies that are designed comply with both ISO 27001:2015 (ISMS) and the Qatar National Information Assurance Policy (NIA) version 2.0.

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.

CONTENTS

PL-IS-02: Information Classification Policy

Contents: • Policy Description • Who Should Know This Policy • Purpose • Scope • Definitions • Policy • Procedures	Version Number:	4
	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
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 a data classification standard.
2. Qatar University commits 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 Policy (NIAP).
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 Policy or equivalent.

7. DECLASSIFICATION

Data declassification can be done either by the owner or by 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.

PL-IS-03: Protection of Intellectual Property Policy

Contents: • Policy Description • Who Should Know This Policy • Overview • Scope • Policy • Policy Sections	Version Number:	4
	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 associated with two main categories of information:

1. Category 1: QU Information, including email and documents.
2. Category 2: The intellectual property of third party organizations, such as software and IT systems and digital resources.

Out of Scope: This policy does not address intellectual property rights for research-related information[1].

5. POLICY STATEMENTS

5.1 QU Information Rights

For the purpose of this policy, "QU Information" includes all information produced in the course of conducting QU business.

1. Qatar University shall retain full ownership and intellectual property rights to QU Information.
2. Employees shall not have the right to claim ownership of QU Information, including unfinished work such as draft documents and all communication related to QU operations.
3. In case of a change of assignment within QU, an individual shall surrender all documents related to their previous assignment to the relevant director or department head. This may include proper disposition of relevant electronic mail according to the best interest of the QU department.

5.2 Third Party Property Rights

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.

[1] See "Intellectual Property Policy and Procedures" issued by the Intellectual Property Advisory Committee endorsed by the Office of the Vice President for Research.

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:	4
	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:	4
	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:	4
• 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 ISO27001:2013 with 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. Information security controls are identified and mandated
5. 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.
6. An agreed upon level of information security and service delivery is defined and is in line with supplier agreements.
7. Monitoring, review and audit of supplier service delivery are conducted regularly.
8. A service management relationship process between ITS and suppliers is defined and assigned to a designated individual or service management team.
9. Appropriate actions are taken when deficiencies in the service delivery are observed.
10. 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.
11. 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.

7. RESPONSIBILITIES

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

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

PL-IS-SG-04: Data Labelling 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

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 Management 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

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.

PL-IS-SG-06: Personnel Security 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

"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:	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

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.

PL-IS-SG-09: Business Continuity Management 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 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.

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

Qatar University 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.

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.

[1] Reference: Qatar National Information Assurance Policy 2.0

PL-IS-SG-11: Data Retention and Archival 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 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, taking into account any requirement for archive copies to be permanently retained. The data retention and archival shall be in compliance with:
    a. University policies and requirements
    b. Regulatory requirements
    c. Legal 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 Proposed Information Privacy & Protection Legislation.
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

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

ITS 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. 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.
7. Any change of an ITS documentation set goes through change control process
8. 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.

9. Documentation sets are reviewed and updated periodically to ensure that they are up to date and current.
10. 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 is in compliance with 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.

[1] Reference: Qatar National Information Assurance Policy 2.0

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.

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, ITS 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, ITS 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-04: Gateway 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

Perimeter gateways acts as the entry point to Qatar University network from Internet. Qatar University, adopts a defense in depth approach to protect against the ever-evolving threats.

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 minimum requirements for securing gateways used for external communications.

4. DEFINITIONS

Gateway	A gateway is defined as any system that interfaces the University's network with the external world, including the Internet and other networks. In terms of this policy, Gateway includes routers, firewalls, content filtering solutions and proxies.

5. POLICY STATEMENTS

The University shall ensure that:

1. Networks are protected from other networks by gateways and data flows are properly controlled.
2. Gateways are hardened prior to any implementation on production site and are protected against:
    a. Malicious code and vulnerabilities
    b. Wrong or poor configurations
    c. Account compromise and unauthorized or inappropriate privilege escalation
    d. Rogue network monitoring
    e. Denial of Service (DoS) attacks
3. Monitoring and supervision of gateways is in place and include threat prevention mechanisms, logging, and alerts.
4. Gateways block or drop any data identified by a content filter as suspicious, including at least the following:
    a. Malware-infected content
    b. Categories of website/content defined as inappropriate in the Cyber Crime Law including sites hosting obscene material, gambling sites, etc.
    c. Denial of Service attacks
5. Data imported to University systems should be scanned for malicious programs.

6. EXCEPTIONS

Exceptions can be defined in case the total cost of applying a security control is more than the asset cost or in case existing technologies Qatar University deployed cannot support the threat vector.

PL-IS-SC-05: Product Security 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 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.
6. 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.
7. Systems comply with all legal requirements including license, copyrights, intellectual property rights, etc.
8. All systems are adequately documented.
9. 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

ITS 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:	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 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:	4
	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.

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	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

Term	Definition
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.

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	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

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 and information processing facilities.
2. Equipment, information or software are not taken off-site without prior authorization.
3. Security is applied to off-site assets taking into account the different risks of working outside the organization's premises.
4. Users ensure that unattended equipment has appropriate protection.

Physical Entry Control

5. IT Facilities are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
6. Physical security for offices, rooms and facilities are designed and applied.
7. Procedures for working in secure areas are designed and applied.

Equipment Security

8. Physical protection against natural disasters, malicious attack or accidents are designed and applied.
9. Equipment are sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
10. Equipment are protected from power failures and other disruptions caused by failures in supporting utilities.
11. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage.
12. Cables are inspected for inconsistencies with the cable register on a regular basis.

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

13. Equipment are correctly maintained to ensure its continued availability and integrity.

Public Access

14. 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

15. 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.

Clear Desk and Clear Screen

16. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted.

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:	4
	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 investigations

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.