Information Technology Policies

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

CHANGE HISTORY

Issue No.	Date	Description of Change
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	Defined additional policies Separated from information security policies
3.1	October 2018	Review by IT Director
3.2	August 2019	Added IT Enterprise Architecture Policy Updated Acceptable Use of IT Resources Policy Updated AUP -> Clear Screen Policy

DISTRIBUTION LIST

This document is controlled by the IT Director, and is available to others as an uncontrolled document.

S/N	Position	Remarks
1	IT Director	Controlled
2	ITS Management	Uncontrolled
3	Qatar University Leadership	Uncontrolled
4	Information Technology Users at Qatar University	Uncontrolled

Contents

Foreword

The Information Technology Services department (ITS) is recognized as the provider of central IT services at Qatar University. Over the past decade, the IT infrastructure and services at QU grew considerably and ITS now provides leading technology solutions that empower its various constituents to excel.

The **academic community** benefits from state of the art classroom technologies, learning management systems, a vast collection of library resources, and a network coverage that extends to all corners of the campus to allow access virtually from anywhere.

For **administrators**, the technology solutions provided by the department are on par with top regional and international educational institutions.

The information security policies included in this document are in line with the following core values:

- **Collaboration:** both within IT and with those we serve—because it helps us understand and support the technology needs of the entire university community.
- **Continuous Improvement:** We strive for operational excellence through the on --- going development of the staff and the organization as a whole.
- **Innovation:** We encourage creative and critical thinking in the development of technology services and solutions.
- **People:** We listen to, respect and care for students, faculty, staff, and one another, both professionally and personally.
- **Service:** We strive to provide excellent service by being consistent, agile, reliable and accessible to all.
- **Transparency:** We leverage open communications and thoughtful business processes to be accountable in our interactions and our work.

Glossary

Term	Definition/Description
BYOD	"Bring Your Own Device" refers to a set of policies, standards, and/or guidelines related to the use of personal devices on corporate networks such as QU.
CMS	Content Management System, typically used to manage the contents of a web site using a user-friendly interface
EBS	Oracle E-Business Suite, the ERP system in use at QU for administrative purposes
ERP	Enterprise Resource Planning system
Information Assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (NISTIR 7298 Revision 2)
Information Security	The protection of all forms of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Adopted from the NIST IR 7298, Revision 2)
IT Security	Technical measures that are implemented to protect the confidentiality, integrity, and availability of digital information assets.
IT Resources	Information Technology resources such as computing devices, network, data, and IT services at QU.
ITS	Information Technology Services Department
ITS Service Desk	Also known as ITS Help Desk. A single point of contacts for all IT related requests for information, services, and assistance.
MFD	A Multi-Function Device that can copy, print, and scan documents to email. These devices support "follow-me" printing, where users can submit a document to be printed and then release it for printing on any of the MFDs that are deployed around campus.
NIAP	Qatar National Information Assurance Policy
QU	Qatar University
QUID	A centrally managed user name used to access IT resources.
SSID	An SSID (Service Set ID) is the name of a wireless network, e.g. "Guest Wireless" or "QU User"
VPN	Virtual Private Network is a technology that allows users to access systems and/or networks that are not directly accessible from the Internet. At QU, the ERP

PL-ITS-02: IT Resources

Contents:	Version Number:	3.1
• 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 expectations of the QU community with respect to information technology resources 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 outline the fundamental services and solutions that the IT Services department should provide to the University community in support of the University's strategy and mandates.

4. Scope

This policy addresses the IT resources provided by the Information Technology Services department (ITS) to Qatar University. This includes, but is not limited, to the following:

1. Physical resources such as:
    a. Computing devices and accessories such as laptops, desktops, tablets, etc.
    b. Telephones, including IP phones and any mobile phones provided by the University.
    c. QU ID cards used to control physical and logical access to various locations and resources on campus.
2. Network access, including wired and wireless access, Internet access, remote access to the internal QU network through VPN (Virtual Private Network).
3. Access to IT services as per the eligibility guidelines for each service, e.g. electronic mail, enterprise resource planning (Oracle E-Business Suite or Banner), learning management systems such as Blackboard, etc.

5. Policy Statements

Qatar University acknowledges the importance of providing technology resources to its community in support of educational, research, and administrative activities. In that regard:

1. The IT Services Department shall provide IT resources to students, faculty, staff and others as needed to fulfill their duties, and in line with the requirements that support the execution of the University strategy.
2. ITS shall maintain and publish a catalog of services that it offers, along with clearly defined service parameters such as eligibility, entitlement, support, related processes and procedures, cost as applicable, etc.
3. Users of QU IT resources are required to comply with the "Acceptable Use of IT Resources Policy".

PL-ITS-03: Acceptable Use of IT Resources

Contents:	Version Number:	3.2
• 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 need to inform QU IT users of restrictions on the use of 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

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

4. Definitions

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

5. Scope

This policy applies to all users of any QU IT resources.

6. Policy Statements

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

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

All users of QU IT resources are required to adhere to the policy sections below.

6.1 General Terms

6.1.1 Acceptable Use

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

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

6.1.2 Prohibited Use

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

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

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

6.1.3 Accountability

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

6.2 Use of Computing Devices

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

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

Users shall not use their computing devices to:

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

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

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

6.4 Use of Electronic Mail

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

1. The use of electronic mail is a privilege extended by QU to its students, faculty, staff and others in order to facilitate communication in the course of conducting University business.

2. The University owns the content of electronic mailboxes of its faculty and staff and all others mailboxes created to facilitate University business, e.g. consultants and contractors.
3. The Information Technology Services Department (ITS) is responsible for managing and supporting the University's email services.
4. ITS may provide access to, or copies of the content of, mailboxes as required by QU business and/or in the course of a security forensic investigation.
5. Email accounts may be disabled:
    a. when an employee's association with the University ends. Exceptions may be granted for a specified period of time if such access is required to fulfill a business need.
    b. if they are linked to security incidents such as SPAM or other inappropriate use of email.
6. **QU employees:**
    a. Shall restrict the use of their QU mailbox to QU-related communication.
    b. Shall not use their QU email address for any personal activities such as registering on online sites.
    c. Shall not forward their QU mail to non-QU systems such as cloud-based email services.
    d. Shall not make offline copies of their mailboxes which may expose them to unauthorized disclosure.
    e. Do not have the right to take copies of their email when their association with the University ends.
7. **All Email Users:**
    a. Shall not share passwords, credit card information, and other restricted data through email without proper protection such as encryption.
    b. Shall not transmit offensive, abusive, violent, threatening and harmful content through email.
    c. Shall not transmit, forward, or post internal emails or attach classified documents containing confidential information to anyone outside of QU.
    d. Shall not transmit, forward, or post chain letter emails to anyone at any time.
    e. Shall not falsify or impersonate a sender address.
    f. Shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of QU or any unit of the QU, while communicating with domains outside QU.
    g. Shall take proper precautions to avoid falling victims for phishing.
    h. Shall not circumvent existing controls for email access.
    i. Shall report any observed irregularities to ITS for further investigation.
    j. May not use mail broadcasting for personal, commercial, and non University-related communication.
    k. Should avoid sending mass emails to users unless content is relevant to all the recipients of the mailing list.
8. Bulk emails and mailing lists:
    a. Mailing lists are provided at Qatar University to facilitate sending emails to a large audience. However users should exercise caution whenever they are sending out bulk emails.

b. Use of bulk email and mailing lists is for University related topics only. Users may not use mail broadcasting for personal, commercial, and non-University related announcements.
c. Communications sent through mailing lists should be targeted to the related audience. Users should avoid sending mass emails to users unless content is relevant to all the recipients of the mailing list
d. Users should consider the content of emails before broadcasting to mailing groups. Users are not allowed to abuse mailing lists by sending unsolicited emails or spam that may contain offensive, threatening or harmful material. In addition, users should not use mailing lists to send advertisements such as advertising a property for sale, car, personal achievement, etc., except through the use of the dedicated mailing list (or group if using the University portal).

6.5 Use of Network and Internet Access

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

1. Users shall not compromise the University resources by knowingly downloading malicious, offensive, abusive, profane, illegal and/or harmful content.
2. Users should refrain from using peer-to-peer file sharing protocols due to the inherent risks associated with such use. Exceptions can be granted following proper assessment and authorization by the Information Security Manager.
3. Users shall not install or configure any active or passive network component without the express consent of ITS. This includes, but is not limited to:
    a. Network access equipment (wired or wireless)
    b. Network servers (e.g. DHCP, DNS, etc.)
    c. Any device that consumes a disproportionate amount of network bandwidth.
    d. Any device that can bypass the security mechanisms enforced by the University.
4. Users shall not bypass the security mechanism implemented and managed by QU for accessing the Internet.
5. Users shall not install devices or software that allow them direct access to their devices or systems without going through the existing security controls such as firewalls or VPN devices. Methods such as modems attached to devices or remote access software such as PCAnywhere can pose a great risk to the QU infrastructure and inadvertently allow perpetrators direct access to internal QU resources.
6. Users are solely responsible for any indirect, consequential, special or punitive damages or losses that may arise from their inappropriate use of the Internet access.
7. Users may submit requests to adjust content filtering or Internet access restrictions from the ITS Service Desk. ITS will assess the risks associated with implementing the request and retains the right to reject any requests that may present a security risk to the University's internal network and/or IT resources.

6.6 Telecommunication Services (Telephones)

QU uses IP phones (hardware and software) to provide telephone services to its employees. Users:

1. Should handle the phones with care and report any hardware or configuration issues to the ITS Service Desk.

2. Should protect their phone PIN, especially if they have access to make long distance calls.
3. Must not abuse their long distance access privileges. Reported abuses may result in disciplinary action.
4. Use emergency phones that are distributed around campus for emergency purposes only.
5. Must return the IP phone hardware to the ITS Service Desk during the exit clearance process.

6.7 Use of Social Media

QU users of social media sites shall NOT:

1. Share QU information through social media platforms.
2. Use their personal accounts to communicate work-related information.
3. Post pictures or information that link them to QU
4. Excessively use social media in the workplace
5. Shall not represent explicitly or implicitly the University on any social media platform without explicit authorization from the University

6.8 Use of Cloud Services

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

6.9 Use of Central File Storage (File Shares)

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

Departmental Shares

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

Individual Shares

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

6.10 Use of QU Web Services

1. Users and web site owners are accountable for any content that they post on QU web servers and that is deemed inappropriate by Qatar University.

2. Data classified as Internal, Limited Access, or Restricted shall not be made available via QU web sites or portal without adequate security controls.
3. Access to the QU portal and other web services shall be terminated when a user's role expires, i.e. the user is no longer a faculty, staff or student at the University. Exceptions are allowed with proper authorization.

6.11 Use of Audiovisual and Classroom Technology

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

1. AV/CT resources may only be used in the course of conducting QU business.
2. In general, only the faculty members are allowed to use the Smart classroom technology system. In case a student requires their use for academic purposes, he should first obtain explicit approval and authorization to do so by the department head where the class is located or by any related faculty member.
3. Users may not attempt to fix any failure of the AV/CT equipment. Instead, they should report such failures to the ITS Service Desk.
4. Users may not at any time try to dismantle and/or move any AV/CT tools without prior authorization from the IT Services Department.
5. Smart classroom technology systems are protected through a PIN code that is provided to initiate access to the tools. The users granted access to that PIN may not share it with others.
6. Students may not use Smart classroom technology systems for non-academic purposes and outside the class hours.
7. The faculty, staff and students may not at any time try to dismantle and/or move any smart classroom technology systems without clearly notifying the ITS Service Desk and obtaining written approval and authorization to do so.

6.12 Use of QU ID Card

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

1. The Card is the property of Qatar University and is non-transferable. A cardholder may allow another person to use the card in case of disability, under the direction and supervision of the cardholder.
2. Possession of the Card by any person other than the owner is a violation of University regulations and can result disciplinary action.
3. Cardholders are required to surrender their Card when it expires, is replaced, or when their association with the University ends.
4. Cardholders must present their Card should be presented upon request by security officers and University administrators, to access campus facilities, to attend events and activities, or to obtain certain services.
5. Depending on the card issuing guidelines, a Card replacement fee applies for cards that are lost or damaged due to neglect or misuse.
6. The University is not responsible for any losses or expenses resulting from the misplacement, theft or misuse of the Card.

7. Cardholders must maintain the Card in its original form with all information clearly visible (i.e. no stickers, punched holes, etc.)
8. Cardholders cannot use the Card as collateral or security for any reason.
9. Cardholders must immediately report a lost or stolen Card to the QU Security Office.
10. If found, lost cards must be returned to the QU Security Office.

6.13 Maintenance of Clear Screen

Users are advised to keep their screen clear of any sensitive information that others may accidently get to see. High windows and/or close them when not in use.

Users shall maintain a clear screen on their desktops/laptops by:

1. Activating the screen saver on their computer
2. Configuring the screen saver to:
    a. lock the screen if the system is idle for more than 5 minutes
    b. require a password to resume operation
3. Not tampering with the screensaver settings enforced by ITS to defeat the purpose of this policy
4. Configuring a screen saver that does NOT display information of personal nature such as a family album.

6.14 Maintenance of Clear Desk

While not purely an Information Technology requirement, users are expected to exercise due care in protecting classified information by:

1. Not leaving any information (paper/books/ledgers) being entered into the system unattended if moving away from the desk even for a short while – like attending a phone call, lunch or break hours etc.
2. Keeping restricted and limited access information protected while entertaining visitors at their desk.

6.15 Expectation of Privacy

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

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

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

6.16 Compliance

Users of QU IT Resources must:

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

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

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

PL-ITS-04: Technical Support

Contents:	Version Number:	3.1
• 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 technical support services provided by the IT Services department related to the use of 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

The purpose of this policy is to define the obligations of the IT Services Department toward supporting end users in using the central QU IT Resources extended to them.

4. Scope

Technical Support services provided by the IT Services Department.

5. Policy Statements

The IT Services department provides services to the University community and ensures that such services are properly managed and supported.

In order to provide an appropriate level of support, ITS may

1. Install a predefined set of software that is necessary to conduct QU business, such as Microsoft Office, anti-malware product(s), management software agents, etc. on end user devices.
2. Enable remote access to end user devices to facilitate technical support personnels' efforts to assist users in resolving technical issues. Such access will always be allowed only after user acknowledgement and acceptance.
3. Collect information necessary to provide the level of support needed, all while preserving the privacy and confidentiality of user documents and activities.
4. ITS reserves the right NOT to support personal devices or software.
5. Users are required to read and acknowledge acceptance of the "Acceptable Use of IT Resources Policy".

Five levels of technical support are available:

1. Level 0: Self-Service
2. Level 1: ITS Service Desk
3. Level 2: In-Depth Technical Support
4. Level 3: Backend Support
5. Level 4: Vendor/Contractor Support

5.1 Level 0: Self-Service Support

Through self-service, end users have access to information and tools that assist them in resolving their immediate problems. To enable this, the IT Services department can provide web-based documents and tools such as:

1. Knowledge base
2. Self-service tools such as the self-service password management tool, EBS and Banner self-service, etc.
3. Request fulfillment through web forms

4. Access to online forums, both internal and external, where users can ask questions or search for solutions.
5. Access to general vendor documentation and tools that can assist end users without the necessity to engage support personnel

5.2 Level 1: ITS Service Desk

The ITS Service Desk (a.k.a. Help Desk) is the first channel of contact for technical support. Service Desk personnel assist users in solving trivial issues and fulfil simple service requests. If no solution is available, the Service Desk escalates the incident or request to a higher support level.

The following services are available through the IT Service Desk:

1. Incident management: to respond to support calls from individual users regarding the use and function of their computing devices and services.
2. Service request fulfillment: to cater to individual service requests such as requesting hardware or software.
3. Knowledge management: to assist end users with simple technology-related tasks. Such assistance may be limited in scope depending on the request.
4. New service requests: to department requests for new services.

5.3 Level 2: In-Depth Technical Support

At this level, experienced and knowledgeable support personnel assess the issues and provide solutions that cannot be handled by Level 1 support. If no solution is available, the issue is escalated further to the next level of support.

The following services are available through Level 2:

1. End user hardware and software distribution and support
2. Application support
3. Audiovisual and classroom technologies support

5.4 Level 3: Backend Support

Level 3 technicians have access to the highest technical resources available for problem resolution, workarounds or developing solutions. They focus on identifying the root cause of a problem and, once identified, provide solutions to resolve it. They then document and share the solutions with level 1 and level 2 personnel.

The following services are available through Level 3:

1. Infrastructure services and support, e.g. database management, network and system deployment and support.
2. Enterprise application support and customization
3. Project management
4. Security services

5.5 Level 4: Vendor/Contractor Support

When all internal resources are exhausted, vendors and/or contractors are engaged to resolve open technical issues. Vendors and contractors are also typically involved in hardware maintenance and support.

The following services are available through Level 4:

1. End user hardware repairs
2. Software development and support, e.g. QU Mobile App
3. Infrastructure hardware repairs, network cabling, Internet access, etc.
4. Response to and collaboration with law enforcement agencies to report and assist in the resolution of security incidents

6. **Exceptions**

Limited or no support of personal computing devices is provided for the following:

1. Non-QU devices
2. Non-standard QU software
3. Devices with non-QU licensed software
4. QU licensed software installed on non-QU computing devices, e.g. assisting students in installing licensed software on their personal computers.

PL-ITS-05: Electronic Mail

Contents:	Version Number:	3.1
• 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 electronic mail at Qatar University.

2. Who Should Know This Policy

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

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

3. Purpose

The purpose of this policy is to ensure that Qatar University electronic mail services is available and reliable, and is used for the purpose of conducting QU business.

4. Scope

This policy applies to all QU email users.

5. Policy Statements

The deployment and use of the QU electronic mail service is governed by the clauses outlined below.

5.1 Individual Email Addresses

1. The Information Technology Services department is responsible for the deployment and management of QU Email services.
2. For QU employees (faculty, staff, consultants, etc.):
    a. Email services are provided to facilitate their QU-related business and operations.
    b. Access to email will be terminated when an employee's association with the University ends.
    c. Email addresses follow a standard format.
3. For students:
    a. The University provides email accounts that remain active after the student's association with the university ends.
    b. QU reserves the right to access and view the contents of a student's mailbox as warranted by local laws and QU policy requirements.
4. Alumni and other users:
    a. Qatar University extends email services to alumni with limited support.
    b. Non-QU users such as consultants and external researchers may get a QU account but such services are governed by the official relationship with the University and will be discontinued after such relationship ends or as required by the concerned business department.
5. Email-related attributes such as addresses and content are the property of the University. As such, QU reserves the right to access and view the contents of mailboxes as warranted by local laws and regulations or QU policy requirements.
6. Mailbox content retention is governed by the overall data retention policy of QU.
7. Restrictions:
    a. QU restricts the mailbox size based the user category. The size of student mailboxes is defined by the contractual agreement between QU and the service provider.

b. QU reserves the right to activate controls to limit the amount of email messages sent from individual accounts to prevent abuse (e.g. outgoing SPAM).

c. Exceptions may be requested and granted based on the business need.

8. The Acceptable Use of IT Resources policy includes additional clauses related to the use of QU Email services.

5.2 Generic Email Accounts

Generic email accounts can be made available to departments to facilitate their operations.

1. QU departments are responsible to assign an "owner" for each of their generic mailboxes who is assigned the responsibility of authorizing access to the mailbox.
2. The department that requests a generic mailbox is responsible for:
    a. The accuracy of the level of user access to the generic mailbox throughout its lifecycle.
    b. Periodic reviews of generic mailbox users and their privileges.
3. Authorized generic mailbox users must use them in accordance with the Acceptable Use of IT Resources Policy.
4. Abuse or misuse of a generic mailbox may result in the mailbox being disabled until a corrective action has been taken.

5.3 Use of Bulk Emails and Mailing Lists:

Qatar University provides mailing list management services in order to facilitate sending emails to a large audience. Users of such services should exercise caution whenever they are sending out bulk emails.

1. The use of mailing list is a privilege extended to campus business units and groups to conduct QU business.
2. Each mailing list shall be assigned an "owner" who is responsible for managing the authorization of the access list and for managing the content of the mailing list.
3. Abuse or misuse of a mailing list may result in the list being disabled until a corrective action has been taken.

6. **Exceptions**

Qatar University may extend email services to external users in compliance with QU policies.

PL-ITS-06: Central File Storage

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

Revision History

No.	Date	Description of Change

1. Policy Description

This policy sets the guidelines governing the use of central file storage facilities.

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 set the rules that govern the deployment, management and use of central file storage services extended to the QU community.

4. Scope

Centrally managed file storage and shares for departments and individual users.

5. Policy Statements

The IT Services department is responsible for managing central file storage services for the University community.

5.1 Individual Shares

The University provides personal file shares for its active constituents, governed by the following:

1. The shares are provided for convenience of individuals and should not be abused.
2. The content of individual shares may not be backed up to central backup facilities. Users are responsible for ensuring that they have additional copies of their stored documents.

5.2 Departmental Shares

1. Departments may request shared file storage, a.k.a. shared folder, to use as a central repository for their documents.
2. Each shared folder must be assigned an "owner" from the requesting department whose responsibilities include:
    a. Being the primary point of contact for ITS within the requesting department
    b. Authorizing access to the shared folder hierarchy
    c. Direct management of user access privileges to the folder, if such capability is granted in agreement with ITS.
3. ITS limits the size of a departmental share based on a balance between business requirements and service capacity parameters.
4. The content of departmental shared folders are backed up on a regular basis.

6. Exceptions

Exceptions to this policy, in particular with regard to extending the standard allocated quota, require the approval of the IT Director.

PL-ITS-07: QU ID Card

Contents:	Version Number:	3.1
• 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 and associated guidelines describe the QU Card along with issues related to governance, services, acceptable use, and guidelines.

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 guidance about the production and use of an identification card on the QU campus.

4. Scope

This policy applies to the production and use of an identification card at Qatar University.

5. Policy Statements

QU ID Card ("Card") issuance and use are governed by the following policy clauses:

1. A Card shall be issued to QU constituents as per the eligibility requirements set forth in the accompanying procedure and guidelines documents.
2. A temporary Card may be issued to non-QU users if required to conduct QU business.
3. Services and benefits that are associated with the use of the Card are subject to compliance with applicable laws, regulations and QU policies and procedures.
4. All Card activities that involve monetary transactions shall be conducted in accordance with the University's financial rules and regulations.
5. All issued Cards are the property of Qatar University.
6. Employees must surrender their Card when their active association with the University ends.
7. An operational guidelines document shall address the following:
    a. Eligibility requirements
    b. Acceptable forms of identification
    c. Applicable fees
    d. Replacement policy and process
    e. Deactivation

PL-ITS-08: IT Project Management

Contents:	Version Number:	3.1
• 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 supports the adoption of a formal project management methodology to manage IT projects.

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 all Information Technology (IT) projects at Qatar University are managed in accordance with a consistent and appropriate methodology throughout the duration of the project so that the deliverables are met on time and within budget, and all IT requests for software and equipment are fulfilled through the appropriate processes and procedures.

4. Definitions

Term	Definition
PMO	ITS Project Management Office
PMM	Project Management Methodology.
EPM	Enterprise Project Management tool
Project Management Methodology	Appropriate management and controls through the four phases of Initiation and Approval, Planning, Execution and Monitor & Control, Closing and Post-Closing
Project	A project is created for the purpose of delivering one or more products, services or results according to a specified business case within a managed environment.
IT Request for Software and equipment	An IT Request can be for Software or Equipment needed by QU as part of a project or as part of QU operational needs.

5. Scope

This policy applies to all IT project management activities conducted at Qatar University.

6. Policy Statements

IT project management activities at QU are governed by the following:

1. The ITS Project Management Office ("PMO") serves as the primary body responsible for managing all IT related projects.
2. The PMO shall adopt a project management methodology (PMM) and adapt it to the specific needs of Qatar University
3. All projects must follow the adopted PMM to ensure that appropriate controls are in place.
4. Information security should be addressed in project management, regardless of the type of the project. The PMM should require that:
    a. information security objectives are included in project objectives;
    b. an information security risk assessment is conducted at an early stage of the project to identify necessary controls;
    c. information security controls are integrated into all phases of the applied project methodology.
5. In special cases the project sponsor or project steering committee can authorize an alternate or varied methodology provided the essential control elements are met.
6. Availability of funding is a pre-requisite to project initiation.

7. Responsibilities

1. The PMO is responsible for oversight of the following:
    a. PMM framework
    b. Providing assistance and expertise to project managers
    c. Project management mentoring and support processes.
2. Project Managers must comply with this policy and are responsible for:
    a. Collaboration with the PMO for training and reporting procedures, and project management policies, processes and procedures.
    b. Identification of and compliance with an established operationally specific methodology:
        i. PMM framework
        ii. Other control processes as determined by the PMO /Project Sponsor / Project Steering Committee.
    c. Accurate reporting to the PMO/project sponsor / project steering committee of matters of significance throughout the project
3. The project sponsor is normally a member of executive leadership within QU who sponsors a project through the initiation and approval phase of the project. The project sponsor's governance and oversight responsibilities for the project may be assumed by a Project Steering Committee.
4. The Project Steering Committee is a group of senior QU executives and leaders (including the Project Sponsor) entrusted with the governance / oversight responsibilities for a project.
5. IT Software or Equipment Requesters must comply with this Policy as well as the IT PMO Procurement and Contracts Policy for appropriate processing of their IT requests for software and/or hardware.

8. Compliance

Failure to comply with this policy may result in delays in project delivery and/or disciplinary action.

9. Exceptions

Exceptions to this policy require the approval of the IT Director.

PL-ITS-09: IT Procurement and Contract Management

Contents:	Version Number:	3.1
• 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 articulates the guiding principles and provisions that apply when procuring IT goods or services for 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 ensure that IT procurement and contract management activities adhere to the following principles:

1. Value for Money
2. Open and fair competition
3. Accountability
4. Risk Management, and
5. Probity and Transparency

This policy must be considered in conjunction with other QU policies, procedures and guidelines.

4. Definitions

Term	Definition
PMO	ITS Project Management Office
EPM	Enterprise Project Management tool
DA	Deliverable Acceptance
RFP	Request For Proposal
RFQ	Request For Quotation
Procurement-related document	RFQ / RFP /License Renewal /Support Renewal
PO	Purchase Order

5. Scope

This policy applies to all IT procurement activities at Qatar University including, but not limited to the following IT-related components:

1. Hardware, software, and services (including cloud services)
2. Consultancy and professional services
3. Contracts, regardless of the total cost

6. Policy Statements

The Information Technology Services department is the central and primary provider of IT services at Qatar University. In order to provide its services in a consistent, efficient, and effective manner, the department manages all IT procurement activities on campus, following recognized best practices and project management frameworks. In that regard:

1. The PMO shall maintain compliance with established QU policies.
2. The PMO may delegate some of the procurement responsibilities to others as deemed appropriate and with the approval of the IT Director.
3. Capital investments in IT resources shall follow the published ITS standards for procurement and project management.
4. ITS shall do due diligence to ensure best utilization of IT resources
5. The procurement of cloud services must undergo risk assessment to ensure the viability and security of the requested service(s).

6. ITS shall establish and maintain a contract and license management system for all IT procurement activities, including monitoring and review of SLAs.
7. ITS can deny implementation or support for IT solutions which have not been properly vetted or which introduce unacceptable risks.

7. Responsibilities

The PMO is the owner of this policy and is responsible for oversight of the procurement cycle.

Project Managers and IT software or equipment requesters must comply with this policy and are responsible for the preparation and submission to the PMO of procurement-related documents including technical and final evaluation reports, project/request deliverable acceptance, etc.

8. Compliance

Failure to comply with this policy can cause delays in IT procurement and/or result in disciplinary action.

9. Exceptions

Exceptions to this policy require the approval of the IT Director.