جامعة قطر
QATAR UNIVERSITY

GU-IS-SG-001

Information Security Guidelines for QU Suppliers

April 2025

DOCUMENT OWNER

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

APPROVAL

	Prepared By	Verified By	Approved By
Name	Mohamad Eljazzar	Divya Mohan	Mohamad Eljazzar
Title	Manager, IT GRC	Senior Risk and Compliance Specialist	Manager, IT GRC
Signature			
Date	12-March-2025	14-March-2025	14-March-2025

CHANGE HISTORY

Issue No.	Date	Description of Change
1.0	14-March 2025	Initial Draft

DISTRIBUTION LIST

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

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

1. Purpose

This document outlines the minimum-security requirements that all suppliers and third-party vendors (hereafter referred to as "suppliers") must adhere to when providing services to Qatar University (QU). The guidelines aim to protect QU's information assets, maintain the confidentiality, integrity, and availability of data, and ensure compliance with international standards and best practices. Suppliers local to Qatar are expected to comply with the local applicable regulations, including those issued by the National Cyber Security Agency (NCSA).

2. Scope

These guidelines apply to all suppliers who:

- Have access to QU's information assets, including but not limited to data, systems, and networks, and/or
- Process, store, or transmit QU's data, and/or
- Provide services that could impact QU's security posture.

3. Requirements

Suppliers must comply with the following security requirements:

3.1 Information Security Management System (ISMS)

Suppliers should implement and maintain an ISMS based on internationally recognized standards such as ISO/IEC 27001 or demonstrate adherence to a comparable security framework.

Suppliers shall provide evidence of their ISMS implementation upon request, which may include certifications, audit reports, or other relevant documentation.

3.2 Data Protection

Suppliers must commit to protecting the confidentiality, integrity, and availability of QU's data in accordance with privacy compliance requirements and best practices.

Suppliers shall implement appropriate technical and organizational measures to prevent unauthorized access, use, or disclosure of data, including:

1. Encryption of data in transit and at rest, using strong encryption algorithms.
2. Strict access controls, including the principle of least privilege and role-based access control.
3. Secure data storage and disposal practices.

4. Regular data backups and disaster recovery procedures.
5. Suppliers shall notify QU immediately in the event of any data breach or security incident.

3.3 Access Control

Suppliers must implement robust access control mechanisms to ensure that only authorized personnel can access QU's information assets.

Suppliers shall:

1. Maintain an access control policy.
2. Identify and authenticate users before granting access.
3. Regularly review and update user access rights.
4. Implement multi-factor authentication where appropriate.
5. Securely manage and protect passwords.
6. Log and monitor access to QU's systems and data.

3.4 Network Security

Suppliers must maintain a secure network infrastructure to protect against unauthorized access and cyber threats.

Suppliers shall:

1. Implement firewalls and intrusion detection/prevention systems.
2. Regularly monitor network traffic for suspicious activity.
3. Apply security patches and updates to network devices promptly.
4. Secure wireless networks, if applicable.
5. Segment networks to isolate sensitive data and systems.

3.5 Vulnerability Management

Suppliers must have a process for identifying, assessing, and remediating security vulnerabilities in their systems and applications.

Suppliers shall:

1. Conduct regular vulnerability scans and penetration tests.
2. Apply security patches and updates in a timely manner.
3. Maintain an inventory of hardware and software assets.
4. Follow secure coding practices for software development.

3.6 Incident Response

Suppliers must have a documented incident response plan to handle security incidents effectively.

Suppliers shall:

1. Establish procedures for reporting and escalating security incidents.
2. Define roles and responsibilities for incident response.
3. Have the capability to contain, eradicate, and recover from security incidents.
4. Cooperate with QU in incident investigations.
5. Notify QU of any security incident that may affect QU’s data or systems, in accordance with contractual agreements and legal obligations.

3.7 Security Awareness and Training

Suppliers must ensure that their employees are aware of their security responsibilities and receive appropriate security awareness training.

Suppliers shall:

1. Provide regular security awareness training to all employees who have access to QU’s information assets.
2. Ensure that employees are trained on relevant security policies and procedures.
3. Promote a culture of security awareness within their organization.

3.8 Compliance with Laws and Regulations

Suppliers must comply with all applicable laws and regulations in the State of Qatar, including but not limited to:

1. The Personal Data Privacy Protection Law
2. Directives and guidelines issued by the National Cyber Security Agency (NCSA), including the Qatar National Cybersecurity Framework (QCSF) and the National Information Assurance Framework (NIAF).

3.9 Audit and Monitoring

QU reserves the right to audit the supplier's security practices and compliance with this document.

Suppliers shall cooperate with QU in any such audits and provide access to relevant information and systems, subject to contractual agreements and legal obligations.

4. Supplier Due Diligence

QU will assess the security posture of potential suppliers as part of the supplier selection process.

Suppliers may be required to complete a security questionnaire, provide evidence of security certifications, or participate in a security assessment.

5. Contractual Agreements

The requirements outlined in this document will be incorporated into contracts and agreements with suppliers.

Non-compliance with the guidelines set in this document may result in termination of the contract.

6. Enforcement

Failure to comply with this guidelines document may result in one or more of the following actions:

- Notification of non-compliance
- Request for a corrective action plan
- Suspension of access to QU's systems and data
- Termination of the supplier contract

7. Review

This document will be reviewed and updated periodically to reflect changes in technology, business needs, and legal and regulatory requirements, including updates to the QCSF and directives from the NCSA.

8. References

Additional references:

- Qatar Personal Data Privacy Protection Law
- Qatar National Information Assurance Standard
- Qatar National Cybersecurity Framework (QCSF)
- Other relevant laws and regulations of the State of Qatar
- QU's Information Security Policy and Handbook