Information Security Policy (ISP)

Contents

1. History of Version

Date	Version	Supervisor	Comments
23/01/2019	1.0	Koljonen, Christina	First Release
31/03/2020	2.0	Senthil Kumar C R	I. Accommodated in the QS UNISOLUTION standard template II. Updated sections: a. Introduction b. Management of Technical vulnerabilities III. Added Revision section
06.11.2020	3.0	Senthil Kumar C R	Formatting of the document and inclusion of GDPR in Section 9.1

2. Introduction

This document outlines the information security policies put in place by senior management of the QS Unisolution. These policies are to be adhered to by all entities included in the QS Unisolution scope

The confidentiality, integrity, and availability of information, in all its forms, are critical to the ongoing functioning and good governance of QS Unisolution. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for QS Unisolution to recover. This information security policy outlines the QS Unisolution approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the QS Unisolution information systems. Supporting policies, codes of practice, procedures, and guidelines provide further details.

QS Unisolution is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity, and availability of data. The principles defined in this policy will be applied to all the physical and electronic information assets for which the QS Unisolution is responsible. QS Unisolution is specifically committed to preserving the confidentiality, integrity, and availability of documentation and data supplied by, generated by, and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001:2013.

3. Revisions

Revisions to this document will be made annually, or whenever deemed necessary.

4. Scope

This policy applies to all locations of QS working for QS Unisolution (referred to as “QSU”), employees of the parent company, and correspondingly freelance individuals working for QS Unisolution (referred to as “Employees “). It also applies to information received from external service providers and/or guests (referred to as “External parties “), to whom non-disclosed information is communicated or made available by QSU. This document will be revised annually or when significant changes occur. No employee is exempt from this policy.

5. Purpose

The purpose of this Policy is to protect the QS Unisolution information assets from all threats, whether internal or external, deliberate or accidental.

The structural elements of this policy:

- Policy context and the objectives defined by senior management.
- System governance and organization for information security of QS Unisolution
- Developed principals and security rules conform to the best practices of information security and are applicable within the entire QS Unisolution.

6. Information Security Policy (ISP)

The Information Security policy statement is detailed in the document “ QSU_ISMS_Manual“. The current policy applies to QS Unisolution including its subsidiaries mentioned in the scope. Information security policy (ISP) rules are required for all employees, suppliers, contractors, subcontractors and users of the QSU's information system, regardless of their activities.

This policy may be supplemented with additional specific policies in relation to commercial offers when appropriate. Supplementary policies define the specific security arrangements put in place to complement the principles and security regulations specified in the ISP.

Exemption of the current security policy may be possible with proper justification validated by senior management and/or the Chief Information Security Officer (CISO).

6.1. ISP Review

At a minimum, the information security policy is reviewed yearly or after significant changes related to

- Organizational, legal, regulatory, contractual and/or technological contexts
- security best practices
- threats and probability feedback
- formal or informal discussions on risk assessments
- improvements resulting from conducted checks and audits.

6.2. Approval

The current Internal policies have been developed by CISO and have been formally approved by senior management. The ISP is communicated to all users that are likely to interact with the QS Unisolution information system. Its application is mandatory and the principle of "need to know" is applied to the communication.

7. Our Organization

7.1. Senior Management

Strategic decisions and matters regarding the security of the information system are handled by senior management. Our Senior management demonstrates leadership and commitment concerning information security by:

- Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of QS Unisolution
- Ensuring the integration of the information security management system requirements into the organization's processes.
- Ensuring that the resources needed for the information security management system are available;
- Communicating the importance of effective information security management and of conforming to the information security management system requirements.
- Ensuring that the information security management system achieves its intended outcome(s).
- Directing and supporting persons to contribute to the effectiveness of the information security management system;
- Promoting continual improvement; and
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

7.2. Chief Information Security Officer (CISO)

Senior management appoints a CISO responsible for information systems security. The CISO plans, coordinates, and monitors all activities related to IS security. The role of the CISO is as follows:

- Lead and coordinate the actions of the group of users associated with information system security.
- Assist and advise about risks and security measures to be implemented during the development of new systems.
- Define and propose means of protection and actions required to achieve security objectives;
- Ensure that solutions are adapted to the issues of security and comply with the requirements of the information security policy;
- Define and consolidate reporting to senior management

7.3. Line Managers

Managers are responsible for the administration and review of access and authorization of users to their services. With the assistance of CISO, assure that their teams are aware of information system guidelines and security policies.

7.4. Data Protection Officer

The Data Protection Officer assures that all necessary measures have been taken by the QSU Group about legal, regulatory, and contractual issues. Regarding information system security, the mission of the DPO is to:

- Keep up to date with judicial standards and jurisprudence, in collaboration with the CISO to communicate and state internal obligations related to information system security
- Ensure compliance with legal, regulatory and contractual provisions concerning information system security;
- In collaboration with the CISO, identify and maintain legal, regulatory and contractual obligations;
- Document and update the procedures used to meet legal, regulatory and contractual obligations;
- Ensure, in collaboration with personnel concerned, the integration of security requirements in contracts with all service providers or external partners;
- Proceed with regular review of contracts.
- Establish legal references.

The DPO plays a supporting role to the various entities. Therefore, the DPO may be consulted when or if further information is required.

7.5. Human Resource

Human resource management shall apply the security rules during the processes of the arrival and departure of employees. Human resource management controls the disciplinary processes related to non-compliance with the QSU Group's practices and security measures.

7.6. Users

Users must comply with all security rules which are communicated to them and report, as quickly as possible, any security incidents, to their Line manager and CISO for further actions.

8. Operations

8.1. Change Management

We aim to prevent malfunctioning of the information system as part of the implementation of changes on platforms (application and system updates, changes in infrastructure, architecture) while maintaining the responsiveness of teams. Security is an integral part of the entire project lifecycle.

8.2. Management of Technical vulnerabilities

Technical vulnerabilities are tested and updated regularly to guard against attacks by correcting known vulnerabilities in systems and applications. Periodic internal and 3rd party (external) penetration testing to assess and analyze the risk of any new vulnerabilities.
External penetration testing covers:

- Web Application Security Assessment
- Web Service Security Assessment
- Security Configuration Review

8.3. Antivirus Protection

We safeguard our information system against viruses and malicious code, protecting vulnerable systems from these threats, as well as information system input and output.

The workstations are equipped with antivirus software of which the antivirus databases are updated by the software provider. Configuration of the antivirus software is managed by the internal IT support team Helpdesk. Users cannot disable, change the configuration, or uninstall the antivirus.

8.4. Backups

In the event of incidents affecting the availability or integrity of assets, we ensure to protect against data loss. Safeguard mechanisms are in place for all systems and data including backups (configuration files, workstation, logs, code, the products concerned: Client data).

8.5. Monitoring and Logging

All critical functions and systems are monitored by Infrastructure support along with data traceability. The Visualizing tool is used to manage log reports and is reviewed regularly.
All the systems and equipment are synchronized to a unique time source. Logs are analyzed by the Infrastructure Head based on abnormality and the legal retention period of logs is consistent with the law. The log reports are stored in protected areas.

8.6. Disposal

All computer equipment containing business information is discarded using a secure erasure process. Paper documents containing sensitive and/ or confidential information are destructed using a Paper shredder as per our Information Security Policy.

9. Compliance

9.1. Compliance to legal, regulatory, and contractual obligations

We respect legal, regulatory, contractual, and various other standards.

The obligations to respect focus notably on the following:

- Local legal and regulatory compliance (E.g GDPR).
- Obligations under standard contracts or conditions of service offerings.
- Obtaining and maintaining certifications recognized under the parameters defined under information security management system ISO/IEC 27001:2013, Cyber risk, etc.

Compliance is practiced through the below measures:

- Up to date legal, contractual and regulatory standards.
- Observation of any developments in the legal, regulatory, contractual, and standards

framework.

- Procedures used to satisfy legal, regulatory, contractual and standards are defined,
- Communication channels are put in place concerning the developments of the framework.
- Monitoring mechanisms can include audit indicators, penetration testing, and vulnerability tests, updates to these tests, and scheduled or annual reviews.
- Action plan for identified non-conformities during audits.

9.2. Security practices

We at QSU adopt the best security practices by defining security rules applicable to the entire information system of QSU Group. Additional security measures identified through risk analysis, legal, regulatory, and/or contractual concerns, and/or specific standards will be addressed accordingly. Statement of applicability shall be created for the applicable controls required for the context of various products like MoveON and MoveIN. Security controls (e.g anonymization and encryption) and best practices shall be considered and implemented as appropriate to the risk level, as mitigation.

9.3. Dealing with Personal data

We have the important responsibility of protecting the personal and sensitive personal data of our clients or prospects by respecting their rights.
Below are the steps ensured at QSU to protect personal data:

- Strong Firewall and Anti-virus: Using multiple layers of security software thus making unauthorized access to client data more difficult
- Access limitation: Changing passwords to key software when an employee departs and protecting the organization's reputation
- Processing information ethically: Being transparent about data collection and usage and adhering to information handling policies
- Data management: Adding value by collecting and managing client data responsibly and strategically
- Training and Education: Training employees on how to handle and interpret client data

10. Dealing with Intellectual Property

We respect Intellectual Property when using software subject to license. The licensed software concerning the information system used within QSU is defined and maintained as part of our Information asset inventory.

The licensing agreements are maintained under the responsible license owner. Requests for installing license software are handled through the proper approval workflow. Regular checks are carried out on the information system to ensure consistency between licensing agreements and current installations.

11. Compliance

Any person, subject to this policy, who fails to comply with the provisions as set out, shall be subjected to appropriate disciplinary or legal action.