qs.com

External

Information Security Policy

1. History of versions

Date	Version	Author	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
27.05.2021	4.0	Senthil Kumar C R	Updates for External Certification Audit 2021
31.08.2021	5.0	Deepali Saxena	QS Rebranding template updated (logo, font etc)
29.03.2022	5.1	Senthil Kumar C R	Mapped to GDPR (EU 2016/679) and European Council, & Commission decision C (2021) 3972 final dated 4.6.2021, included EDPB measures

2. Reference

ISO 27001	ISO 27018	SURF (CPB/WPB)	GDPR/BDSG
5.2			GDPR Chapter IV and Chapter V

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

External

Table of contents

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

3. Introduction

This document outlines the information security policies put in place by senior management of the QS Unisolution (QSU). The ISMS Policy below is supported by various subordinate policies, procedures, guidelines, templates, and checklists

QS Unisolution - ISMS Policy

We at QS Unisolution shall continuously strive to enhance competitiveness of our customers with a range of value-added products and provide world class support to the Institutions at large by adopting a process approach to excellence.

This would be enabled by implementing an Information Security Management System, with involvement of relevant stakeholders for:

- Ensuring enhanced customer experience & meeting applicable requirements
- Proactively protecting & ensuring security of data and information assets
- Fulfilling compliance obligations with respect to privacy & security
- Ensuring information security through Design, Risk management, Change Management & ISMS Controls
- Continually improving the information management system and processes.

This policy and supporting policies are part of the ISMS 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 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 as documented in QSU's Information Security Management System (ISMS) 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

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

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 and applicable legal/regulatory compliance requirements, specifically GDPR (EU 2016/679).

4. Revisions

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

5. 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 Clients (referred to as "Controllers"), external service providers and/or guests (referred to as "Sub-processors" or "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 & contractors are exempt from this policy.

6. 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.

7. Information Security Policy

The Information Security Policy statement as provided in Section 1 above is applies to QS Unisolution including its subsidiaries mentioned in the scope. Information security policy are required to be understood and underlying QSU ISMS implemented for all employees, sub-processors, suppliers, contractors, sub-contractors, 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 and measures define the specific security arrangements put in place to complement the principles and security regulations specified in

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

the policies. GDPR requirements e.g., Data Processing Agreements (Art.28), Technical and Organization Measures (Art.28 & 32), Data Protection Impact Assessment (Art.35), Records of processing activities (Art. 30) etc. shall be ensured through ISMS procedures and controls, as per the Statement of Applicability.

7.1. Policies 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 vulnerabilities
- Discussions on ISMS risk assessments
- Changes to ISMS
- Improvements resulting from periodic reviews and audits.

7.2.Approval

The ISMS policies have been developed by business, process owners and reviewed by CISO and have been formally approved by the respective policy owners/senior management. The policies are communicated to all users that are likely to interact with the QS Unisolution information system and Its application is mandatory.

8. QS Unisolution organisation

8.1. Senior Management

Strategic decisions and matters regarding the privacy and security requirements for the information system are managed 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

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

information security management system.
- Promoting continual improvement.
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

8.2.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 periodic reporting to senior management (Management Review Meeting- MRM)
- Responsible for Information Security Management System implementation
- Makes periodical review and updates on ISMS process to ensure the efficiency and effectiveness of information security controls
- Communicating Regular updates on changes to legislation, internal ISMS process or methods to employees
- Monitoring Information Security Incidents and take appropriate actions
- Evaluating compliance with the company processes through regular Internal Audits
- Organization of information security trainings for all employees
- Organizing security awareness campaigns to enhance the security culture and develop a broad understanding of the ISMS requirements
- Ensuring that internal audits are periodically conducted, and action items are taken to closure.
- Appropriate contacts with relevant authorities (regulatory, legal) must be maintained.
- Providing a vision to the organization from a security standpoint.

8.3. 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.

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

8.4. 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
- Monitors compliance with GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
- Ensure compliance with legal, regulatory, and contractual provisions concerning information system security.
- In collaboration with the CISO & privacy officer, 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.
- Cooperates with the supervisory authority
- Contact point for the supervisory authority on issues relating to processing, including the prior consultation and to consult, where appropriate, about any other matter
- The DPO plays a supporting role to the various entities. Therefore, the DPO may be consulted when or if further information is required.
- Ensures to have due regard to the risk associated with processing operations, considering the nature, scope, context, and purposes of processing.

8.5. Human Resource

Human resource management shall apply the security rules during the processes of the arrival and departure of employees according to the ISO 27001 control A 7. Human resource management controls the disciplinary processes related to non-compliance with the QSU Group's practices and security measures.

8.6. 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.

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

9. Operations

9.1. 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. Risk Management process is invoked to support the change management process.

9.2.Management of Technical vulnerabilities

As per a risk-based approach, technical vulnerabilities are evaluated and updated regularly to guard against attacks by correcting known vulnerabilities in systems and applications. Periodic internal and third party (external) penetration testing is conducted to assess and analyse the risk of any new vulnerabilities.
External penetration testing covers:

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

9.3. Antivirus Protection

QS safeguards its information system against viruses, malicious code attack, Cyber-attack protecting vulnerable systems from these threats, as well as information system input and output.

The QS staff systems are equipped with antivirus software, the software provider updates the antivirus databases periodically after reviewed with QS corporate IT. Configuration of the antivirus software is managed by the QS corporate IT support -helpdesk. Users cannot change the configuration or uninstall the antivirus.

9.4. 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 (Application configuration, Application source code, Application logs, Access logs, Database logs, configuration files, code, product databases supporting Client data). Business continuity plans are in place and regularly evaluated.

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

9.5. 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.

9.6. 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. Procedures are established for secure disposal of information security assets. A data retention policy is established for normal working. In case of client data, applicable contractual and legal/regulatory requirements are ensured.

10. Compliance

10.1. Compliance to legal, regulatory, and contractual obligations

We respect legal, regulatory, contractual, requirements and adopt applicable standards.

The key drivers and mechanism include the following:

- Local legal and regulatory compliance requirements (E.g., for GDPR, these include related data processing agreements and standard contractual clauses as per European Council, & Commission decision C (2021) 3972 final dated 4.6.2021 and related EDPB guidelines).
- Obligations under standard contracts or conditions of service offerings.
- Obtaining and maintaining certifications recognized for information security management system ISO/IEC 27001, Cyber risk, etc.

Compliance is ensured through:

- Up to date legal, contractual, and regulatory requirements and measures as per European Council, & Commission decision C (2021) 3972 final dated 4.6.2021 and related EDPB guidelines.
- Observation of any developments in the legal, regulatory, contractual, and standards framework.
- Procedures and their implementation to satisfy legal, regulatory, contractual and standards,
- Communication channels in place concerning the developments of the framework.

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

- 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.

10.2. Security practices

QSU adopts the best security practices by defining security controls applicable to the entire information system of QS Group. Additional security measures identified through risk analysis, legal, regulatory, and/or contractual concerns, and/or specific standards -shall be addressed accordingly. Statement of applicability -is established for the applicable controls required for the context of various products like MoveON and MoveIN that enable Software as a Service (SaaS) offerings. Security controls and best practices -are be considered and implemented as appropriate to the risk level,

10.3. 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:

- ISO 27001 Controls adopted and implemented per the Statement of Applicability
- Technical and Organisational Measures as required by GDPR and as per European Council, & Commission decision C (2021) 3972 final dated 4.6.2021
- Strong Firewall and Anti-virus: Using multiple layers of security software thus making unauthorized access to client data more difficult
- Access control: Purpose based access provision as per a strong password policy, which ensures changing of passwords to key software systems and immediate access revocation in cases when an employee exit
- Processing information ethically: Being transparent about data collection and usage and adhering to information handling policies
- Regular compliance checks against applicable regulations like GDPR
- Data management: Adding value by collecting and managing client data responsibly and strategically, as per contractual and legal/regulatory obligations
- Training and Education: Training employees on ISMS, GDPR and Cyber security to enhance the focus on how to manage personal data and maintain confidentiality

11. 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 managed through the proper approval workflow. Regular

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

checks are conducted on the information system to ensure consistency between licensing agreements and current installations.

12. Compliance

Compliance Checks and Internal External Audits are established to verify legal compliance and ISMS process conformance. Sub-processors and or/any person, who fails to comply with the QSU ISMS and legal compliance requirements, shall be subject to appropriate disciplinary and/or legal action.

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com