SQ-POL-009

INFORMATION & DATA SECURITY POLICY

Document No.	Revision	Effective Date	Status
SQ-POL-009	00	30.08.2026	APPROVED

1. Purpose and Commitment

SafeQult Consulting recognises information and data security as an important element of professional and responsible service delivery.

In the course of our activities, we may process information belonging to clients, business partners and SafeQult Consulting, including operational and technical documentation, reports, personal data and other confidential information.

Our objective is to protect information against unauthorised access, disclosure, alteration, loss or destruction and to maintain an appropriate level of its confidentiality, integrity and availability.

2. Scope

This Policy applies to information and data processed by SafeQult Consulting regardless of its format or location.

This includes electronic documents and files, email and electronic communications, paper documentation, client and project data, reports, photographs and working materials, personal data, devices used for business activities, and IT systems and services used to store or transmit information.

3. Information Protection Principles

Information should be protected according to its nature, sensitivity and the potential consequences of loss, alteration or unauthorised disclosure.

SafeQult Consulting applies a risk-based approach considering confidentiality, integrity and availability of information.

4. Access Control

Access to information should be limited to persons who require it to perform their responsibilities or a specific assignment.

Access rights should be appropriate to responsibilities and limited to the minimum necessary. User accounts, passwords and other authentication credentials should not be shared with unauthorised persons.

Where available and justified by the level of risk, additional security measures such as multi-factor authentication should be used.

5. Passwords and Authentication

Passwords used to protect systems and services should be appropriately strong, unique and protected against disclosure.

The same password should not be used across multiple important services where this could increase the risk of unauthorised access. Authentication credentials should be changed where compromise or disclosure is suspected.

6. Devices and Software

Devices used to process information related to SafeQult Consulting activities should be appropriately protected against unauthorised access.

Depending on device capabilities and the level of risk, appropriate measures should include access protection, automatic device locking, operating system and software updates, protection against malicious software, and encryption where available and justified.

Unauthorised or untrusted software should not be installed on devices used to process business information.

7. Storage and Transmission of Information

Information should be stored and transmitted using solutions appropriate to its nature and level of confidentiality.

Before sending documents or data, recipients, attachments and the scope of information being shared should be verified. Confidential information should not be transmitted using casual or unauthorised communication channels.

Access to client documentation should be limited to what is necessary for the relevant assignment.

8. Backups and Data Loss

Appropriate measures should be used to reduce the risk of permanent loss of information important to business continuity.

The scope and frequency of backups should reflect the importance of the data and the ability to recover it. Backup copies should be protected against unauthorised access.

9. Remote Work and Mobile Devices

Particular care should be taken to protect devices and information when working remotely, travelling or carrying out assignments on vessels, installations or client locations.

Devices should not be left unattended where unauthorised persons could gain access. Processing or discussing confidential information should be avoided where it could be intercepted, viewed or overheard by unauthorised persons.

10. External Providers and Services

Where external services are used to store, process or transmit information, they should be selected with consideration of the nature of the information and associated risk.

Information shared with external providers should be limited to what is necessary. Where an external provider processes personal data on behalf of SafeQult Consulting, the requirements of SQ-POL-006 Privacy Policy also apply.

11. Information Security Incidents

Suspected loss of a device or data, unauthorised access, disclosure of information, malware infection or another information security incident should be appropriately reported and assessed without undue delay.

Action should be taken to limit the consequences of the incident, secure affected information and systems, prevent further unauthorised access, establish the scope and cause of the incident, and implement appropriate corrective actions.

Where an incident involves personal data or client information, applicable legal, contractual and notification obligations should also be considered.

12. Information Retention and Disposal

Information should not be retained longer than required for its purpose, applicable legal or contractual obligations, or legitimate business needs.

At the end of the appropriate retention period, data and documents should be securely deleted, destroyed or anonymised depending on their nature. Personal data retention is also addressed in SQ-POL-006 Privacy Policy.

13. Confidentiality

Confidential information should be handled in accordance with SQ-POL-008 Confidentiality Policy.

The obligation to protect information continues after completion of an assignment or business relationship where the information remains confidential.

14. Awareness and Responsibility

Information security depends not only on technology but also on the behaviour of persons who have access to information.

Anyone processing information in connection with SafeQult Consulting activities should exercise appropriate care, protect authentication credentials and report identified threats or incidents.

15. Our Commitment

SafeQult Consulting is committed to applying practical and proportionate information protection measures appropriate to the nature of its activities and associated risks.

Information security should be considered when using technology, communicating, storing documentation and working with clients and business partners.

Information security does not depend on technology alone. It starts with the responsible handling of information.

APPROVAL

Prepared / Approved by	Role	Date	Signature
Przemysław Łobocki	CEO	30.08.2026