1 General

RISCO Group takes and has for many years taken a practical and analytical approach to Information Security. Security Policies and Procedures have been developed in parallel and in conjunction with the best practices in the industry. The resulting policies are documented in this document, and all other related documents as part of the ISMS.

2 Leadership and commitment

RISCO Group's Senior management shall demonstrate leadership and commitment with respect to the information security management system by:

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

RISCO Group's CISO and senior management are in charge or creating and updating the ISMS, so it will:

1. Be appropriate to the purpose of RISCO Group;
2. Provide the framework for setting information security objectives;
3. Include a commitment to satisfy applicable requirements related to information security;
4. Include a commitment to continual improvement of the information security management system.
5. Be available as documented information;
6. Be communicated within RISCO Group;
7. Be available to interested parties, as appropriate.

3 Information Security Policy

This Information Security Policy is the top-level statement of the RISCO Group information security hierarchy. It is considered to be the basis for all RISCO Group information security regulations.

This Information Security Policy defines information security as the protection of information from loss of confidentiality, integrity and/or availability. The scope of this Policy includes all information which is stored, processed, transmitted or printed using any system or storage medium. The Policy applies to all RISCO Group staff and to all other individuals who directly or indirectly use or support the services or information of RISCO Group or any of its operating entities.

3.1 Policy Objective

The purpose of this policy is to document overall objectives and RISCO Group security drivers. This information security policy defines guidelines for the proper use and protection of RISCO Group's resources and all data stored on these resources.

This group-wide security policy forms the general framework and guideline for all security-related activities within RISCO Group. It contains a definition and explanation of general security-related terms and defines the principal processes, responsibilities and dependencies of information security.

3.2 Policy Scope

The scope of this policy includes all information which is stored, processed, transmitted or printed using any system or storage medium of RISCO Group. The policy applies to all RISCO Group staff and to all other individuals who directly or indirectly use or support the services or information of RISCO Group or any of its operating entities.

- All persons described will be required to agree to adhere to the terms of this policy.
- A review of this policy occurs at least every year.
- All modifications must be documented in the document history with the responsible author, date and subject.
- The RISCO Group Chief Information Security Officer (CISO) is responsible for this policy.

3.3 Context

This information security policy defines the framework for all security-related processes and documents RISCO Group. It constitutes the top level of the hierarchy described and defines security objectives, asset classification and responsibilities for securing these assets in accordance with the business goals.

3.4 Objectives

3.4.1 Information Security Building Blocks

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

The protection will be achieved by keeping in mind the following basic components when designing every IT system or process: Confidentiality, Integrity and Availability (CIA).

IT Security is based on the following building blocks:

- Confidentiality

  The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

  Examples:
    - Protection of user account credentials
    - Protection of sensitive information
- Integrity

  The property of safeguarding the accuracy and completeness of assets.

Examples:

- Protection from the manipulation of Sensitive information.
- Protection from the manipulation of systems (e. g. through viruses, Trojan horses)

- Availability

The property of being accessible and usable upon demand by an authorized entity.
Examples:

- Reliability during the service provision
- Access to information on schedule

- Non-Repudiation

The ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.

Examples:

- Proof-strong comprehensibleness of user transactions

Integration of These 3 components and the non-repudiation objective in every business procedure or IT system will increase the level of information protection that system provides.

3.4.2 The Information Security Policy objectives

RISCO Group information security policy set the appropriate policies that will be based on the information security building blocks and will assure:

- Confidentiality

  To ensure that information will not be disclosed to anyone who is not authorized to access it. The confidentiality of information, including transaction and processing, must be safeguarded by appropriate measures in respect to protection and classification.
- Integrity

  To ensure that all information is accurate and complete. The quality of information processing must be maintained at all times. It must be possible to verify the integrity of data at any point during the processing phase.
- Availability

  To ensure that all information is available when required. The availability of IT as a whole, as well as the functioning of specific services, must be guaranteed according to the priorities which have been defined.
- Audit Information

  IT-related processing must be traceable by means of logging relevant information. The audit trail shall allow information sources to be validated and track any system changes made. Events putting the security of IT systems at danger must trigger immediate action.
- Security Concepts

  Based on a risk analysis, adequate information security measures are defined. Details of the scope and level of information security measures implemented must be documented in a complete, clear and up-to-date manner. The measures must adhere to cost/benefit principles. Any remaining risk must be identified and brought to the attention of the senior management. This will ensure that the residual risk remains within acceptable limits.
- Maintaining Information Security

  Information security must be constantly reviewed, updated and adapted in line with changing conditions and technology, whilst taking into account changes in the level of risk and in security mechanisms.

Therefore, it is essential that:

- All information is protected against unauthorized access by members of RISCO Group, contractors or other individuals from outside RISCO Group;
- All information is adequately protected against corruption or loss during input, processing, transmission or storage.
- All information and information systems which are essential to the activities of RISCO Group have to be adequately protected in respect to the level of IT services required.
- Awareness of the need for information security as an integral part of the day-to-day operation of business systems has to be created and maintained. This ensures that all employees understand the importance of information security, their own responsibility for security and the effects of security upon the financial success of RISCO Group.
- All staff has to be aware of and comply with relevant internal and external rules relating to the maintenance, protection and withholding of information.

4 Policy Fundamentals

Information must be protected in such that:

- Privacy is protected in accordance with the RISCO Group's Privacy Policy or other local privacy regulations
- Information confidentiality is preserved.
- The integrity of all information is guaranteed.
- Information is available as necessary
- Transactions cannot be repudiated
- Legal and contractual obligations can be fulfilled.

It is required that:

- For every piece of information (data, procedures and supporting systems), an information owner is appointed
- The security scope is justified in relation to the value associated with the information and the related business risk
- Users are responsible for the correct handling of all information
- It is possible to audit all transactions
- There is an independent examination of the administration and use of information.
- Preventive measures must have priority over reactive damage control. Where possible, security measures shall be supported or enforced by technical solutions.

5 Support and Operation

5.1 Resources

RISCO Group shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

5.2 Competence

RISCO Group Management shall:

1. Determine the necessary competence of person(s) doing work under its control that affects its information security performance;
2. Ensure that these persons are competent on the basis of appropriate education, training, or experience;
3. Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;
4. Retain appropriate documented information as evidence of competence.

5.3 Awareness

Each internal or external employee or any other person doing work for RISCO Group control shall be aware of:

1. This policy;
2. Their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance;
3. The implications of not conforming with the information security management system requirements.

5.4 Communication

RISCO Group shall determine the need for internal and external communications relevant to the information security management system including:

1. On what to communicate;
2. When to communicate;
3. With whom to communicate;
4. Who shall communicate;
5. The processes by which communication shall be effected.

5.5 Operation

RISCO Group shall:

1. Plan, implement and control the processes needed to meet information security requirements
2. Keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
3. Control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
4. Ensure that outsourced processes are determined and controlled.

6 Detailed Security Policies & Responding Control Objectives

RISCO Group has established policies used to implement effective ISMS within the group. These policies respond to the ISO 27001 (2013 version) controls and controls objectives as follows:

(7.5) Documents management policy

RISCO Group will manage and control the documentation effectively, and provide the necessary guidelines required to control the related ISMS documents effectively.

(9a) Internal Audit

RISCO Group shall review of the implementation and effectiveness of the RISCO Group ISMS and conduct internal audits at planned intervals to ensure the information security management system conforms to RISCO Group's own requirements for its information security management system.

RISCO Group shall Plan, establish, implement and maintain an audit program, define the audit criteria and scope for each audit, Select auditors and conduct audits to ensure objectivity and the impartiality of the audit process, ensure that the results of the audits are reported to relevant management and Retain documented information as evidence of the audit program and the audit results.

(9b) Management Review

RISCO Group shall conduct management reviews of the information security management system (ISMS) at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

(10) Continual improvement

RISCO Group shall continually improve the suitability, adequacy and effectiveness of the information security management system (ISMS).

The senior management is in charge of promoting continual improvement and providing the resources needed for continual improvement.

A.6a Organization of information security

RISCO Group shall define the organizational model for comprehensive information security management for RISCO Group, this includes defining the objectives, interfaces and responsibilities for information security management in accordance to the relevant international standards.

RISCO Group CISO is responsible for the protection of RISCO Group assets, carrying out specific security processes, information security risk management activities and acceptance of residual risks.

The Information Security Top Management Forum shall be comprised of top management and the CEO shall perform as the Forum's chairman.

The Information Security Committee shall be comprised of knowledgeable managers / employees from relevant departments. The CISO shall perform as the committee's chairman and determine its agenda according to the necessary needs.

Appropriate contacts with relevant authorities / special interest groups, shall be maintained.

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the RISCO Group's assets.

A.6b Mobile devices and teleworking

RISCO Group shall ensure the security of teleworking and use of mobile device.

When using mobile devices, special care should be taken to ensure that RISCO Group's information is not compromised. Each mobile device user should take into account the risks of working with mobile devices in unprotected environments.

Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

A.7a Human resource security

RISCO Group shall ensure that employees who access RISCO Group's information will go through the appropriate human resources process throughout all of their stages of employment.

RISCO Group shall provide the security guidelines for the employees and managers of RISCO Group related to HR processes including training and define the security measures that must be obeyed by all RISCO Group employees and contingent workers, while working with any IT system.

RISCO Group should ensure that employees, contractors and external party users understand their responsibilities and are suitable for the roles they are considered for.

For each new candidate for employment, background verification checks shall be carried out proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
As part of their contractual obligation, employees shall agree and sign the terms and conditions of their employment contract, which shall state their and RISCO Group's responsibilities for information security.
RISCO Group shall ensure that employees and external party users are aware of and fulfill their information security responsibilities.
Management shall require all employees and external party users to apply security in accordance with established policies and procedures of RISCO Group.
All employees of RISCO Group, and where relevant, external party users, shall receive appropriate awareness program, education and training and regular updates in RISCO Group policies and procedures, as relevant for their job function.

RISCO Group shall have a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

RISCO Group shall protect its interests as part of the process of changing or terminating employment.

A.7b End User Policy

RISCO Group shall establish a contractual obligation with employees as part of their employment contract, which shall state their and RISCO Group responsibilities for information security.

Security guidelines for the users of desktop or laptop computers from an end user perspective shall be documented.

RISCO Group shall define the security measures that must be obeyed by all RISCO Group employees and contingent workers, while working with any system.

A.8 Asset management

RISCO Group shall achieve and maintain appropriate protection of organizational assets.

All RISCO Group's assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

RISCO Group should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion, destruction, protection. Documentation should be done in dedicated or existing inventories as appropriate.

Assets maintained in the inventory should be owned. Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.

Rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented and implemented.

RISCO Group Information shall be classified, to ensure that information receives an appropriate level of protection in accordance with its importance to RISCO Group. Information classification is the responsibility of the information owner and the classification may vary by each operating entity.

Media handling shall be managed, to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

A.9a Access Control

RISCO Group shall restrict access to its information and information processing facilities, ensure authorized user access and prevent unauthorized access to systems and services.

RISCO Group shall make users accountable for safeguarding their authentication information and prevent unauthorized access to systems and applications.

User registration and de-registration should be implemented for granting and revoking access for all user types to all systems and services. Users shall be required to follow RISCO Group's security practices in the use of secret authentication information. The allocation and use of privileged access rights shall be restricted and controlled.

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9b Password Policy

RISCO Group shall establish documentation and guidelines for the use of passwords.

Passwords must never be written down or stored in an unprotected fashion. A user's personal password must never be stored on any kind of media.

Users must be able to change their own passwords. Passwords complexity must be enabled using the capabilities provided by the specific technology being implemented. All accounts must age and expire passwords within the limits imposed by the Password Management Standard.

A.10 Cryptography

RISCO Group shall ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.

Standardization of cryptographic protocols shall help ensure interoperability and help preserve the availability of sensitive information assets.

Cryptographic keys should be managed though their whole lifecycle including generating, storing, retaining, retrieving, distributing and retiring and destroying keys.

All RISCO Group code delivered to customers must be digitally signed using the RISCO Group IT approved service.

A.11 Physical and environmental security

RISCO Group shall prevent: unauthorized physical access, damage and interference to its information and information processing facilities, loss, damage, theft or compromise of assets and interruption to its operations.

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information or information processing facilities. RISCO Group's secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. RISCO Group's equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. Equipment, information or software should not be taken off-site without prior authorization.

Security Manager working with the appropriate business and functional partners shall understand the risk associated with all RISCO Group operations within their scope of responsibility.

A.12 Operations Security

RISCO Group shall ensure correct and secure operations of information processing facilities, ensure that information and information processing facilities are protected against malware and loss of data.

RISCO Group shall record events and generate evidence, ensure the integrity of operational systems, prevent exploitation of technical vulnerabilities and minimize the impact of audit activities on operational systems.

Operating processes and procedures should be documented and made available to all users who need them.

Changes to the organization, business processes, information processing facilities and systems shall be controlled. The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

RISCO Group shall ensure that information and information processing facilities are protected against malware. Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Backup copies of information, software and system images should be taken and tested regularly in accordance with the backup policy.

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

RISCO Group shall ensure the integrity of operational systems.

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, RISCO Group's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A.13a Network security management

RISCO Group shall ensure the protection of its information in networks and its supporting information processing facilities. RISCO Group shall determine the controls required to ensure the protection of information in networks and the protection of the supporting infrastructure, and establish guidelines for the security of all networks that managed, run or used within RISCO Group.

RISCO Group's networks shall be managed and controlled to protect information in systems and applications.

Groups of information services, users and information systems should be segregated on networks.

Planning processes must be based on secure, future-oriented technologies.

Network addresses must only be issued by the relevant network managers.

Cables must be laid in such a way as to prevent information being subject to eavesdropping using the radiation affecting adjacent installations such as heating pipes or power cables. A plan shall be created that gives detailed information on the routing of lines, or indicates which rooms accommodate network components revealing the sensitive points of a network, and is thus in particular need of protection.

Wherever it is required to use encrypted network protocols instead of clear-text protocols, encrypted protocols must be used.

Suitable measures must be taken in order to prevent disaster and to ensure the business continuity in the case of an emergency.

A.13b Information transfer

RISCO Group shall maintain the security of information transferred within RISCO Group and with any external entity.

Agreements should address the secure transfer of business information between RISCO Group and external parties.

Information involved in electronic messaging should be appropriately protected.

A.14 System acquisition development and maintenance

RISCO Group shall ensure that security is an integral part of information systems across the entire lifecycle.

RISCO Group shall ensure that information security is designed and implemented within the development lifecycle of information systems, and the protection of data used for testing.

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

No new software may be put into use unless an IT security concept for this software has been designed and implemented.

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development efforts.

RISCO Group shall establish and appropriately protect secure development environment for system development and integration efforts that covers the entire system development lifecycle. Tests of the security functionality shall be carried out during development.

A.15 Supplier relationships

RISCO Group shall ensure protection of its information that is accessible by suppliers and maintain an agreed level of information security and service delivery in line with supplier agreements.

Information security requirements for mitigating the risks associated with supplier access to RISCO Group's information or information processing facilities shall be documented.

RISCO Group should regularly monitor, review and audit supplier service delivery.

A.16 Information security incident management

RISCO Group shall ensure a consistent and effective approach to the management of information security incidents, and provide the necessary guidelines required to effectively and efficiently respond to computer security incidents.

Information security events shall be reported through appropriate management channels as quickly as possible.

Employees and external parties using RISCO Group's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

A.17 Information security aspects of business continuity management

RISCO Group shall ensure that information security continuity shall be embedded in its business continuity management (BCM).

RISCO Group shall ensure protection of information at any time and the availability of information processing facilities.

Any infrastructure and business process considerations, should include requirements for information security and continuity of information security management in adverse situations.

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

All RISCO Group entities must prepare for disasters by working out disaster plans for all IT systems in use. Whenever new systems are introduced, the disaster planning must be updated or extended.

Disaster plans must list and describe roles and responsibilities in case of a disaster.

A.18 Compliance

RISCO Group shall ensure that information security is implemented and operated in accordance with RISCO Group's policies and procedures, and avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

Information systems should be regularly inspected for compliance with RISCO Group's information security policies and standards.

All relevant statutory, regulatory, contractual requirements and RISCO Group's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system.

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with statutory, regulatory, contractual and business requirements.

Privacy and protection of personally identifiable information should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

Cryptographic controls should be used in compliance with all relevant agreements, laws and regulations.