

Information Security Policy

Document ID	ISMS_PL_Information_Security_Policy
Document status	Draft
Version	3.1
Creator / Owner	CISO
Approver	CEO
Valid from / Issued	16.5.2025
Electronic Location	Resco main web page (Trust Center)
Security Classification	PUBLIC

Contents

1	Introduction	2
1.1	Purpose	3
1.2	Context and Requirements.....	3
1.3	Scope.....	4
1.4	Objectives.....	4
1.5	Referenced Documents.....	6
1.6	Abbreviations.....	7
2	Information Security Principles.....	8
3	Roles and Responsibilities.....	9
3.1	CEO.....	9
3.2	All employees/contractors	9
3.3	Chief Information Security Officer (CISO).....	10
3.4	Security Engineer/Analyst.....	10
3.5	Process Area Managers	11
3.6	IT Manager (Internal IT and Production IT)	12
3.7	Information Governance Board.....	13
3.8	Human Resources	14
4	Contact with Relevant Authorities.....	15
5	Contact with Special Interest Groups.....	16
6	Relevant Legislation and Regulation	17
7	Review and Continuous Improvement	17
8	Information Security Policy – Exceptions.....	18
9	Associated Documentation	18
	Appendix A – Resco Departments and Process Areas	19

1 Introduction

1.1 Purpose

This information security policy describes Resco's approach to information security management.

It provides the guiding principles and responsibilities necessary to protect the security of all Resco operations. Supporting policies and procedures provide further details, see references [1]-[32].

The purpose of Information Security for Resco is to protect information assets, regardless of whether these are held in manual or electronic form.

Implementation of this policy shall provide assurance to interested parties (see chapter 5), that their information is held securely and used appropriately.

1.2 Context and Requirements

Resco develops mobile solutions integrated with CRM Servers from industry's global players (e.g. Microsoft and Salesforce) as well as implements and operates CRM Software-as-a-Service solutions based on Resco Cloud.

Resco has customers and partners all over the world and offices in 3 different countries:

- Bratislava, Slovakia (Headquarter)
- Trebišov, Slovakia (Sales)
- Brookline, MA, United States (Sales)

Resco's departments and processes are described in Appendix A of this document.

The main requirements for the implementation of an Information Security Management System are:

- The necessity to protect the information assets of Resco as well as its partners and customers.
- Responsibility of Resco to operate in accordance with European Union and Slovak legislation, as well as with the Microsoft Supplier Privacy & Assurance Standards (for further details, see chapter 6).

1.3 Scope

Resco is committed to a robust implementation of Information Security Management in accordance with the security standard ISO/EC 27001:2022 and the Microsoft Supplier Data Protection Requirements.

Resco's Information Security Policy applies to:

- All business process areas of Resco, all office locations, all departments.
- All Resco's information, information owned by its clients and partners, and information about its clients.
- All Resco's personnel, and third parties who have access to Resco premises, systems or information.
- All Resco's systems, software, and other information.

It also includes the requirement to comply with any criminal and civil law, statutory, regulatory or contractual obligations, and any other security requirement, including business continuity management.

Non-compliance with this policy is dealt with Resco's HR Disciplinary Process [21] and may result in disciplinary action, termination of contract, or criminal prosecution in the most serious of cases.

1.4 Objectives

Resco's information security policy was implemented to ensure the following three main objectives:

- Confidentiality
Resco's data and information assets are limited to people who have authorized access and are not disclosed to others.
- Integrity
Resco's keeps data intact, complete and accurate, and internal and external IT systems operational.
- Availability
Resco's information and systems are available for all stakeholders (employees, partner, customers and external authorities) when needed.

In particular, personal information shall be handled in accordance with the European Union General Data Protection Regulation (GDPR) and other applicable regulations (see chapter 6).

1.5 Referenced Documents

Reference	Document Information	Issue Date
[1]	ISMS Manual	Latest version
[2]	Information Classification Policy	Latest version
[3]	Asset Management Policy	Latest version
[4]	Access Control Policy	Latest version
[5]	Mobile Device Policy	Latest version
[6]	Backup Policy	Latest version
[7]	Password Policy	Latest version
[8]	Acceptable Use Policy	Latest version
[9]	Supplier Security Policy	Latest version
[10]	Cryptographic Control Policy	Latest version
[11]	Anti-Malware Policy	Latest version
[12]	Physical Security Policy	Latest version
[13]	Network Security Policy	Latest version
[14]	Operations Security Policy	Latest version
[15]	Segregation of Duties Policy	Latest version
[16]	Security Incident Management Policy	Latest version
[17]	Data Protection Policy	Latest version
[18]	Security Risk Management Procedure	Latest version
[19]	General Management Procedure	Latest version
[20]	HR Exit Management Procedure	Latest version
[21]	HR Disciplinary Process	Latest version
[22]	HR Talent Acquisition	Latest version
[23]	Software Development Procedure	Latest version
[24]	Internal Audit Procedure	Latest version
[25]	Corrective Actions Procedure	Latest version
[26]	Document Control Procedure	Latest version
[27]	Change Management Procedure	Latest version
[28]	Patch Management Procedure	Latest version
[29]	Supplier Security Assessment Procedure	Latest version

[30]	Project Management Handbook	Latest version
[31]	Security Incident Response Plan	Latest version
[32]	Disaster Recovery Plan	Latest version
[33]	Monitoring changes of legal requirements procedure	Latest version
[34]	Cloud Service Policy	Latest version

1.6 Abbreviations

Abbreviation	Description
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
IGB	Information Governance Board
ISMS	Information Security Management System
DPO	Data Protection Officer

2 Information Security Principles

The following information security principles apply for the management of information security at Resco:

1. Resco shall implement an Information Security Management System (ISMS) which is compliant with ISO 27001:2022. The implementation of the ISMS shall consider the requirements of relevant authorities and special interest groups and shall be done based on industry best practices. Resco shall analyze which of these requirements will be addressed through the ISMS.
2. Resco shall develop a comprehensive set of policies and procedures to support this Information Security Policy. The policies and procedures shall include, but are not limited to, the referenced documents [1] – [34] in section 1.5.
3. Information shall be classified according to an appropriate level of confidentiality, integrity and availability. When classifying information, the relevant legislative, regulatory and contractual requirements shall be considered [2].
4. Resco employees with responsibilities for information shall ensure the classification of that information is defined [2].
5. All Resco employees must handle information appropriately and in accordance with its classification level.
6. Information shall be both secure and available to those with a legitimate need for access in accordance with its classification level. Access to information will be managed on the basis of least privilege given the need to know [4].
7. Information shall be protected against unauthorized access and processing in accordance with its classification level.
8. Violations of this policy shall be reported.
9. Information security policies shall be regularly reviewed at least once per year, including through the use of annual internal audits.
10. To ensure that the objectives of information security are achieved, Resco shall implement process success criteria and process controls in accordance with such criteria.
11. The principles of continuous improvement, as described in ISO27001, clause 10, shall be applied to Resco's Security Information Management System. Changes to the ISMS shall be carried out in a planned manner.

3 Roles and Responsibilities

This chapter outlines the roles and responsibilities for information security at Resco. The ISMS Manual [1] and supporting policies and procedures [2] – [34] describe the roles in more detail.

A detailed table of role and responsibility definitions is specified in the ISMS_PD_Responsibility_Assignment_Matrix.

3.1 CEO

In the context of Information Security, Resco's CEO is responsible for (also see [19]):

- Definition of goals and the scope of the Information Security Management System
- Providing direction and active leadership for activities in relation to the Security Information Management System.
- Specification of Resco's operating strategy in the context of data protection
- Definition of roles & responsibilities related to Information Security
- Provision of resources and budget approval
- Management and supervision of Resco's external communication
- Conducting reviews of the Information Security Management System with the objective to continuously improve it.
- Overall risk acceptance [18]

3.2 All employees/contractors

All Resco's employees and contractors are responsible for ensuring that they conduct in conformance with the policies and procedures of Resco's Information Security Management System. All employees and contractors must familiarize themselves with this policy and its supporting policies and procedures. Compliance with the policies and procedures of Information Security is mandatory – failures to comply are subject to disciplinary actions.

In particular:

- Act in conformance with the Acceptable Use Policy [8], the Mobile Device Policy [5], and the Anti-Malware Policy [11].

- Report Security Incidents and Data Breaches without delay and according to the applicable policies [16], [17].

3.3 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) coordinates Resco's activities related to information security management. Main responsibilities are:

- Definition of the Information Security Management System
- Coordinating all activities related to the ISMS
- Communication of information relating to ISMS in the Organization
- Communication with relevant authorities and groups of interest in the area of ISMS
- Coordinating Resco's risk management process
- Plans and conducts internal audits related to Information Security. Audits are conducted with respect to Resco's Information Security Management System and the conformance with ISO/IEC 27001 controls.
- Plans, prepares and conducts trainings related to information security (in particular Security Awareness training).
- Yearly review of all Information Security policies and procedures.

3.4 Security Engineer/Analyst

The scope of work for a Security Engineer involves a wide range of responsibilities aimed at safeguarding the organization's information systems, data, and infrastructure from cybersecurity threats such as:

- Designing, implementing, and maintaining security infrastructure, including firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, and security information and event management (SIEM) systems.
- Monitoring security events and alerts generated by security systems to detect and respond to potential security incidents.
- Conducting investigations into security breaches, incidents, and suspicious activities to determine root causes and recommend remediation actions.
- Identifying, assessing, and prioritizing vulnerabilities in IT systems and applications through vulnerability scanning and penetration testing.

- Coordinating with system administrators and developers to implement patches, updates, and security fixes to mitigate vulnerabilities.
- Enforcing least privilege principles and ensuring proper authentication and authorization mechanisms are in place.
- Developing, implementing, and enforcing security policies, standards, and procedures aligned with industry regulations (e.g., GDPR, HIPAA, PCI DSS) and best practices.
- Conducting compliance assessments and audits to ensure adherence to regulatory requirements and internal security standards.
- Developing incident response plans and procedures to effectively respond to and recover from security incidents.
- Conducting digital forensics investigations to collect and analyze evidence related to security breaches and incidents.
- Providing security awareness training and education programs to employees to raise awareness of cybersecurity threats, best practices, and organizational security policies.
- Creating security awareness materials, such as training modules, newsletters, and posters, to promote a culture of security within the organization.
- Performing risk assessments and risk analysis to identify, assess, and prioritize security risks to the organization's IT assets and operations.
- Developing risk management strategies and controls to mitigate identified risks and vulnerabilities effectively.
- Collaborating with architects, system administrators, and developers to design and implement secure IT architectures, systems, and solutions.
- Reviewing and evaluating proposed IT projects and initiatives from a security perspective to ensure security requirements are adequately addressed.
- Staying informed about the latest cybersecurity threats, trends, and technologies through ongoing research, training, and professional development.
- Continuously evaluating and improving security processes, procedures, and controls to enhance the organization's overall security posture.

3.5 Process Area Managers

- Resco's process area managers are responsible for implementing compliant procedures within the business area of their responsibility.

- Ensure that information is classified and handled according to the Information Classification Policy [2].
- Process area managers are asset owners and ensure that the Asset Management Policy [3] and Access Control Policy [4] is adequately implemented within their area of responsibility and that risks to assets are identified and managed according to the Security Risk Management Procedure [18].
- Implement appropriate segregation of duties according to the Segregation of Duties Policy [15].
- Provide training to their team members and ensure that team members comply with the ISMS and with the Acceptable Use Policy [8].
- Taking disciplinary actions (supported by Human Resources) in terms of misconduct.

3.6 IT Manager (Internal IT and Production IT)

Have the same generic responsibilities as process area managers. In addition:

- Ensure that a mobile device management system is implemented to support the Mobile Device Policy [5].
- Ensure that asset management and access management are properly implemented for all IT systems and services according to Asset Management Policy [3] and Access Control Policy [4].
- Ensure that cryptographic controls and procedures for key management are implemented according to the Cryptographic Controls Policy [10].
- Ensure that operational procedures are implemented according to the Network Security Policy [13] and Operations Security Policy [14], Anti-Malware Policy [11], Cloud Service Policy [34], and Password Policy [7].
- Ensure that Change Management [27] and Patch Management [28] procedures are followed.
- Ensure that the Segregation of Duties Policy [15] is implemented for privileged access and activities.
- Ensure that IT suppliers conform with the requirements outlined in the Supplier Security Policy [9].

- Ensure that management of technical vulnerabilities and incident response procedures are implemented according to the Information Security Incident Management Policy [16].
- Ensure that backups are planned, scheduled and tested according to the Backup Policy [6].
- Ensure that Disaster Recover procedures are implemented and tested according to the Disaster Recovery Plan [32].

3.7 Information Governance Board

Resco established an Information Governance Board (IGB) with the following members:

- CEO
- Chief Information Security Officer
- Security Engineer
- Operations Manager
- Legal Manager
- HR Manager

The Information Governance Board is the forum where all topics related to Information Security are addressed to be solved in a coordinated manner.

The Information Governance Board acts as audit committee when audit results are presented, and risk treatments actions are decided upon.

IGB Meetings

The IGB meets at least once per month with the following default agenda:

1. Assess Minutes and Actions from last meeting
2. Review of Risk Register (new risks / changes of context)
3. Review progress of Risk Treatment Plan
4. Track and analyze security incidents (security incident log)
5. Review and track progress of ISMS Implementation

Regular meetings of the IGB shall be formally documented (meeting minutes).

3.8 Human Resources

- Responsible for employees' awareness and compliance with information security.
- Defining the employee lifecycle from recruitment [22] till exit in conformance with Resco's information security requirements [20].
- Supporting managers while taking disciplinary actions in terms of misconduct [21].

4 Contact with Relevant Authorities

The relevant authorities related are:

National Security Authority of Slovak Republic (NBU)

<https://www.nbu.gov.sk>

Office for Personal Data Protection of the Slovak Republic

<https://dataprotection.gov.sk/uouu/>

For the requirements of the relevant authorities, also see chapter 5.

Resco shall implement and document procedures for communicating with the authorities.

In particular, the communication in case of security incidents [16] and data breaches [17] shall be implemented and documented.

5 Contact with Special Interest Groups

The following stakeholder groups are interested in Resco's Information Security Management System:

Interested Party	Requirements
Resco's employees and Resco's business process areas	Protection of their information and personal data
Resco implementation partners	Protection of their information and Personal Data
Resco customers	Protection of their information and Personal Data. In particular, information handled in Resco's mobile applications and Resco Cloud services shall be adequately protected.
National Security Authority of the Slovak Republic "Národný bezpečnostný úrad" (NBU) https://www.nbu.gov.sk	Compliance with law 69/2018 "Zakon o kybernetickej bezpečnosti" ENISA guidelines for the implementation of minimum security measures for digital service providers
Office for Personal Data Protection of the Slovak Republic Úrad na ochranu osobných údajov Slovenskej republiky https://dataprotection.gov.sk/uouu/	Secure processing of Personal Data
Microsoft	Microsoft Supplier Data Protection Requirements (SSPA program)
ISO 27001 Auditor (TUV SUD)	Conformance with ISO 27001:2022

Resco's CISO is responsible for identifying the interested parties and their requirements.

Resco's CISO is responsible for communication with the interested parties and shall develop communication procedures which include how to communicate.

Resco's DPO is responsible for communication with the Office of Personal Data Protection of the Slovak Republic

6 Relevant Legislation and Regulation

Resco's ISMS shall be designed and implemented to be compliant with the requirements in the following legislation and regulation:

- Slovak Republic laws:
 - 69/2018 Z. z. - Zákon o kybernetickej bezpečnosti
 - 452/2021 Z. z. - Zákon o elektronických komunikáciách
 - 366/2024 Z. z. - Zákon, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti"
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT (General Data Protection Regulation)
 - Slovak Republic law: "Zákon č. 18/2018 Z.z. o ochrane osobných údajov"
- ISO/IEC 27001:2022 and ISO/IEC 27002:2022
- Microsoft Supplier Privacy & Assurance Standards (SSPA),
- Microsoft Supplier Data Protection Requirements (DPR)

Changes in legal requirements shall be regularly monitored and transferred into business processes [33].

A list of all legislative regulations that affect the organization is provided in the current version of the register of legal regulations
IS_PD_Register_of_legal_requirements.

7 Review and Continuous Improvement

The Information Governance Board (IGB) will review this policy on a yearly basis or on the event on particular changes of Resco's context and requirements.

The results of the review will be documented and translated into actions for continuous improvements.

The Information Security Officer will plan internal audits according to the Internal Audit Procedure [24]. To ensure independence, internal audits shall be outsourced to third parties as required.

Results of corrective actions will be planned and implemented according to the Corrective Action Procedure [25].

8 Information Security Policy – Exceptions

Resco does not intend to permit any exceptions related to this policy.

However, all exceptions must be requested with enough detail and mitigation controls before they can be decided upon by the Information Governance Board.

Resco CISO is responsible for maintaining a register of all approved exceptions.

9 Associated Documentation

This policy is supported by a comprehensive set of policies and procedures which build Resco's Information Security Management System. This includes all documents referenced in section 1.5 of this policy.

10 Appendix A – Resco Departments and Process Areas

CEO	General Management
Sales	Direct Sales
	Partner Sales (Microsoft)
	Partner Sales (Salesforce)
Partners Channel	Partner Channel
Marketing	Marketing (Website operations, external marketing agencies, marketing campaigns)
Legal	Legal Operations
Finance Internal Operations Unit	Finance and Accounting
	Budgeting and Controlling
	Travel Management
Office Management Internal Operations Unit	Office operations
	Entrance system, security
	Mobile Devices
Software Development	Software Development
	Software Testing
	Build Management
HR	Talent Management
	Recruitment and Exit Management (incl. onboarding)
	Learning and Development (incl. training)
	Internal Communication
	Compensation & Benefits (incl. payroll & docs)
	Performance Management
Internal IT Internal Operations Unit	Internal IT
	Teleworking, external systems
Production IT	Operations of customer facing IT systems and services: Resco Cloud, Websites, Amazon and Azure environments
Product Support	Product Support (Maintenance)
Product Management	Product Management
Project Management	Project Management
Information Security	Information Security Management System, Data Protection