

Information Security Policy

Rail Solutions Group B.V.

31 October 2025

Table of Contents

1. Information Security Policy	4
1.1 Introduction	4
1.2 Objectives	4
1.3 Scope	4
1.4 Policy Statement	4
1.5 Responsibilities	5
1.6 Enforcement.....	5
1.7 Standards	5
2. Data Ownership and Classification Policy	6
2.1 Purpose	6
2.2 Policy Responsibilities	6
2.3 Assignment of Ownership	7
2.4 Data Classification	7
2.5 Measures for Data Protection.....	8
3. Systems and Networks	9
3.1 Prohibited Activities	9
3.2 Physical Security	9
4. Electronic Mail (Email) Policy	10
4.1 Ownership	10
4.2 Usage Rules	10
4.3 Personal Use	10
4.4 Compliance	11
5. Internet Security	11
5.1 Purpose	11
5.2 Ownership and Monitoring	11
5.3 Usage.....	11
5.4 Non-Business Browsing.....	11
6. User Management	11
6.1 System Access	11
6.2 Identification	12
6.3 Verification and Authentication	12
6.4 Authorization	12
6.5 Termination of Access	12
6.6 Additional Access Controls	12

7. Password Policy	12
7.1 Purpose	12
7.2 Ownership	12
7.3 Administration	13
7.4 Configuration Standards	13
7.5 Maintenance	13
7.6 Critical Passwords	13
7.7 Monitoring	13
7.8 System Enforcement	13
8. Clean Desk and Computer Use	13
8.1 Clean Desk Standards.....	14
8.2 Computer Use	14
9. Portable Media and Equipment.....	14
9.1 Key Requirements	14
10. Destruction of Media and Equipment	15
10.1 Media Disposal.....	15
10.2 Equipment Disposal	15
11. Anti-Virus Protection	15
11.1 Implementation	15
12. Intrusion Prevention	15
12.1 Physical Security.....	15
12.2 Logical Security	15
13. Training and Awareness	16
13.1 Purpose	16
13.2 Scope.....	16
13.3 Content	16
13.4 Incident Response.....	16
13.5 Continuous Improvement	16

1. Information Security Policy

1.1 Introduction

This policy establishes comprehensive guidance for the secure use of company technology, including email, internet access, laptops, and portable devices. All computer hardware, software, operating systems, storage media, and network accounts used for email, web browsing, or file transfer—together with associated documentation such as reports—are the exclusive property of the Company. These resources are provided strictly for legitimate business purposes in support of the Company's operations and the interests of its clients and partners.

1.2 Objectives

Information security is a critical business asset of the Company. Appropriate measures must therefore protect all data—digital, physical, or network-based—from loss of **confidentiality, integrity,** or **availability.**

This policy aims to maintain these three essential principles:

- **Confidentiality** – Information is accessible only to authorized individuals.
- **Integrity** – Information remains accurate, complete, and protected from unauthorized alteration.
- **Availability** – Information and systems remain accessible to authorized users whenever required.

1.3 Scope

This policy covers all information processed, stored, or transmitted by the Company, in any medium or format. It applies to every employee, contractor, consultant, and any other individual performing work on behalf of the Company, regardless of location or employment status.

1.4 Policy Statement

The Company is committed to maintaining a secure information environment by ensuring that:

- Information is protected against unauthorized access or disclosure.
- Confidentiality, integrity, and availability are preserved at all times.
- All relevant legal, regulatory, and contractual obligations are met.
- Business-continuity and disaster-recovery plans are developed, tested, and maintained.
- Information-security awareness is promoted among all staff.
- Actual or suspected breaches are reported immediately and investigated by designated personnel.
- Intellectual-property and copyright laws are respected.

- Systems are safeguarded against malicious code and cyber threats.

1.5 Responsibilities

The **Chief Executive Officer (CEO)** and **Compliance Officer** hold primary responsibility for maintaining this policy and providing overall direction and guidance on information security. The **Chief Technology Officer (CTO)** and departmental management are responsible for enforcing this policy within their areas of control and ensuring that employees understand their obligations.

Employees must:

- Exercise sound judgment in using Company resources and seek clarification when uncertain.
- Conduct themselves ethically and protect data obtained through their role.
- Avoid exploiting or attempting to exploit system weaknesses.
- Perform duties diligently and remain accountable for the appropriate use of computing assets.
- Seek clarification regarding data classification whenever confidentiality is uncertain.
- Report any violations, weaknesses, or suspicious activity to the designated security personnel or their line manager.
- Cooperate with investigations and follow the Incident-Response Procedure.

1.6 Enforcement

Failure to comply with this policy will trigger a management review and may lead to disciplinary action in accordance with the Company's disciplinary procedures.

1.7 Standards

All supporting standards, procedures, guidelines, and operating instructions form part of the **Corporate Information Security Framework**. These documents are binding and will be implemented by the CEO and CTO. Compliance will be monitored through regular audits and reviews.

2. Data Ownership and Classification Policy

2.1 Purpose

Data represents one of the Company's most critical assets and must be managed with integrity, accountability, and respect for legal obligations. Establishing a robust data-classification framework ensures that every category of information receives an appropriate level of protection in proportion to its sensitivity and regulatory impact.

Equally important is the clear assignment of responsibility so that these safeguards are applied, monitored, and continuously improved across all business areas.

2.2 Policy Responsibilities

Data Owners

- Are accountable for identifying and classifying all data within their area of control.
- Determine the appropriate security controls according to the assigned classification.
- Ensure that controls remain compliant with legal, regulatory, and contractual obligations.
- Hold exclusive authority to grant, modify, or revoke access rights to that data.

Data Custodians / Processors

- Are responsible for safeguarding data that has been entrusted to them, in any format, for the duration of their custodianship.
- Must apply technical and organizational measures that maintain confidentiality, integrity, and availability.
- Typically include IT Support or infrastructure personnel who maintain the systems storing or processing the data.

Data Users

- Receive access privileges from the relevant Data Owner solely for business purposes.
- Must use data only within their authorized scope and never exceed or misuse granted permissions.

Management

- Designates Data Owners and Data Custodians after evaluating data sensitivity and operational roles.
- Ensures all involved personnel understand their obligations through communication, training, and periodic review.

2.3 Assignment of Ownership

The Company retains ultimate ownership of all data generated or processed within its environment.

Operational responsibility and decision-making authority may be delegated to specific departments or roles to ensure effective management. Data ownership is therefore a **shared accountability model**—encompassing governance, stewardship, and protection—rather than a single point of possession.

2.4 Data Classification

This policy establishes the Company's adherence to a formal **Data-Classification Standard**. It defines employee responsibilities for implementing that standard and provides guidance for categorizing information assets according to their confidentiality, regulatory exposure, and business value.

Classification	Description	Data Type
Confidential	Data whose loss, corruption or unauthorised disclosure would be a violation of laws and regulations, even if the disclosure is only internal within the Company.	Sensitive employee data includes information such as criminal records, medical histories, and political affiliations. Sensitive customer data comprises employee payroll details, banking information, employment contracts, non-public financial data of the company, user credentials, business strategies, intellectual property, confidential source code, CCTV recordings, and office alarm codes.
Secret	Data that, if lost, corrupted, or disclosed without authorization, could harm the company's business operations, image, reputation, or research capabilities, and potentially lead to financial or legal losses. This data constitutes the primary focus of the company's operations and is typically familiar to employees within specific departments or projects.	Source code, marketing strategies, essential customer details, fundamental employee records, and data stored on the intranet server within departmental or segregated directories.
Internal	Information intended for general employee awareness. Data where potential loss, corruption, or unauthorized disclosure would	Information stored in public folders on the intranet server, the internal directory of contact information, company policies and procedures, and guidelines.

	not inherently lead to business, financial, or legal repercussions.	
Public	Data that does not fit into any of the other specified data classifications below. This information can be publicly released and shared with third parties.	The company's registered location, permit and license details, publicly available website content, marketing materials, and press releases.

Data should be classified as **Confidential**, **Restricted**, or **Internal** wherever applicable. **Public** information does not require classification labeling. This categorization framework is not exhaustive, and additional data types may fall under any of these classifications based on sensitivity and risk. In cases of uncertainty regarding the appropriate classification, the information must be treated as **Confidential** by default until formally reviewed and confirmed by the designated Data Owner.

2.5 Measures for Data Protection

Class	Measures	Type of Authorisation Required
Confidential	Data must be encrypted using the most robust techniques available for both storage and transmission. Additionally, networks or databases containing such information should be isolated from other networks.	Access to this information, whether by third parties or internal personnel, must always adhere strictly to a need-to-know and least privilege basis, approved by the data owner.
Secret	It should be subjected to the same level of control as internal data. Moreover, if this data is transmitted over a public network, it must be encrypted to maintain confidentiality. All data transmissions must be encrypted at all times.	Access to this information by third parties must always be granted strictly on a need-to-know and least privilege basis, approved by either the data custodian or the data owner. Internal access will follow the same criteria and may be authorized by a line manager or department head.
Internal	The availability and integrity of the data must be safeguarded during both transmission and storage. Encryption is not mandatory for internal transmission, but access to this data must be controlled through authentication measures.	Third-party access necessitates permission from the data custodian or data owner. Internal users do not require authorization for disclosure.
Public	Does not require specific protection measures during storage or transmission.	No authorization is necessary for internal or third-party disclosure.

3. Systems and Networks

Authorized Company personnel may monitor equipment, systems, and network traffic at any time to maintain security and performance. While the Company strives to uphold a reasonable level of privacy, all information created, transmitted, or stored on Company systems remains the property of **Rail Solutions Group B.V.** Users should therefore have no expectation of absolute confidentiality when using Company resources. The Company reserves the right to conduct regular network and system audits to verify compliance with this policy and relevant laws.

3.1 Prohibited Activities

Without explicit written authorization, the following actions are strictly forbidden:

- Violating intellectual-property rights, including installing or distributing unlicensed or “pirated” software.
- Copying or digitizing copyrighted material (text, photos, music, or software) without authorization.
- Exporting software or technology in violation of export-control regulations.
- Introducing or spreading malicious code such as viruses, worms, Trojans, or email bombs.
- Sharing account credentials or permitting anyone—including household members—to use a Company account.
- Transferring Company or client data between office and personal devices without management approval.
- Using Company resources to access, transmit, or store material that violates harassment, discrimination, or obscenity laws.
- Making fraudulent or misleading commercial offers on behalf of the Company.
- Issuing warranties or representations except where explicitly part of assigned duties.
- Performing or facilitating network intrusions, data theft, denial-of-service attacks, or other disruptions.
- Conducting port or vulnerability scans without prior written approval.
- Intercepting or monitoring network traffic not intended for the user’s device.
- Circumventing authentication or other access-control mechanisms.
- Intentionally disrupting another user’s service or terminal session.
- Using scripts or commands to disable, overload, or interfere with systems.
- Disclosing internal directories or employee information to unauthorized third parties.
- Removing, tampering with, or granting unauthorized physical access to Company equipment.

3.2 Physical Security

Strong access-control and environmental safeguards must protect all Company facilities and equipment.

- Premises must have structurally secure walls, doors, and windows.

- At the end of each business day, all access points must be locked and alarms activated by the final person leaving.
- Visitors must remain escorted at all times.
- Core infrastructure must be hosted in an **ISO/IEC 27001-certified** data center providing environmental protection, power redundancy, and 24 / 7 monitoring.
- Office servers must be housed in locked, hazard-free rooms and maintained regularly.
- Network and power cabling must be protected against interference and damage.
- Backup media must be stored securely away from heat, moisture, and magnetic fields.

4. Electronic Mail (Email) Policy

Email is provided to facilitate official business communication. This section outlines responsibilities for employees who create, send, or receive messages through Company email systems.

4.1 Ownership

All email infrastructure, content, and attachments created or transmitted via Company systems are the property of **Rail Solutions Group B.V.** The Company may access or disclose such content when required for regulatory, legal, or operational reasons.

4.2 Usage Rules

- Apply the same professionalism and tone used in formal written correspondence.
- Do not send Confidential or Restricted data in plain text; approved encryption must be used.
- Do not transmit copyrighted or proprietary material without authorization from the Compliance Officer or relevant Manager.
- Do not use Company email for religious, political, or personal solicitation.
- Refrain from forwarding jokes, chain letters, or mass mailings, especially to external recipients.
- Forward suspected virus or phishing alerts to IT for verification before distribution.
- Avoid downloading attachments or clicking links from unverified sources.
- Never execute attachments containing executable code (.exe, .vbs, .com, .swf).
- Do not send offensive, harassing, or discriminatory content.
- Do not read or access messages not addressed to you unless formally authorized.
- Do not conceal identity or impersonate another user.
- Posting to forums, chatrooms, or social-media sites using Company email addresses requires management approval.

4.3 Personal Use

Occasional, limited personal use of email is permitted if it does not interfere with job performance or breach this policy. All such communications remain subject to Company monitoring.

4.4 Compliance

Non-compliance may result in disciplinary action, including termination or legal proceedings. Employees must immediately report suspected misuse; whistleblower confidentiality will be maintained whenever possible.

5. Internet Security

5.1 Purpose

Internet access is provided solely to conduct legitimate business on behalf of the Company. All usage must comply with internal policies and applicable law.

5.2 Ownership and Monitoring

The Company owns all computer and network infrastructure, software, and stored data. To maintain security, the Company may inspect devices, network logs, and internet activity. Employees must promptly report any violation to Information-Security staff; reporter confidentiality will be protected.

5.3 Usage

- Only Company-approved browsers, software, and gateways may be used.
- Encrypt sensitive data during transmission.
- Accessing illicit, hacker, or suspicious websites is prohibited.
- Downloading or installing executable software without authorization is forbidden.
- Browsers automatically record visited sites; users must not attempt to delete or obscure logs.
- Security personnel performing vulnerability testing must first obtain written approval and use isolated systems containing no production data.

5.4 Non-Business Browsing

Limited personal browsing may occur during breaks, provided all other usage rules remain observed.

6. User Management

User-access management ensures that only authorized individuals obtain system access appropriate to their role, minimizing the risk of unauthorized intrusion or misuse. This policy applies to all users—employees, contractors, and third parties—who require access to Company systems or data.

6.1 System Access

All users must log in using a unique User ID and a password or passphrase. Authentication must succeed before system interaction.

6.2 Identification

Each User ID must uniquely identify one individual and must never be shared or reused. Access is granted only after proper verification and managerial authorization.

6.3 Verification and Authentication

User identities must be authenticated before system access. Multi-factor authentication (MFA) should be implemented wherever possible, particularly for privileged or remote accounts.

6.4 Authorization

Access is granted on the principles of **least privilege** and **need-to-know**. Managers must:

- Define required resources and specific permission levels (read, write, execute).
 - Use standardized naming conventions for users and resources.
 - Periodically review access rights and remove unnecessary privileges.
- Administrative commands may be executed only by authorized personnel.

6.5 Termination of Access

Upon employee or contractor separation, the CTO (or delegate) must promptly disable all accounts and notify any external platforms to which access was granted. Relevant correspondence and data shall be archived according to retention policy.

6.6 Additional Access Controls

Dormant Accounts – Disable or change credentials for default vendor accounts and unused profiles.

Automatic Log-off – Workstations must lock after 30 minutes (or less) of inactivity; back-office systems must log off after 60 minutes.

Failed Login Attempts – Lock or throttle accounts after 3–6 unsuccessful attempts depending on risk level; automatic re-enablement is prohibited.

7. Password Policy

7.1 Purpose

Passwords are critical for verifying identity and controlling access. They must be created, used, and maintained securely at all times.

7.2 Ownership

Each user holds exclusive ownership of their password and is responsible for keeping it confidential. Password sharing or reuse is prohibited.

7.3 Administration

Users must:

- Choose complex passwords meeting configuration standards.
 - Change initial credentials upon first login.
 - Report any suspected compromise immediately.
- Administrators must enforce technical password controls across systems.

7.4 Configuration Standards

- Minimum of 8 characters.
- Include at least three of four character types: uppercase, lowercase, numbers, symbols.
- Avoid dictionary words or predictable sequences.
- Use password managers where approved.

7.5 Maintenance

- Change every 60 days for high-risk systems; every 120–180 days for others.
- Do not reuse passwords until at least four unique changes have occurred.
- Never record passwords in plain text.
- Vendor default passwords must be replaced immediately.

7.6 Critical Passwords

The CTO and IT Support maintain sealed, emergency copies of administrative passwords (firewalls, backups, servers). These are stored securely under dual authorization and accessed only in emergencies.

7.7 Monitoring

Authorized staff may perform periodic password-strength audits using approved tools. Weak passwords must be changed immediately.

7.8 System Enforcement

Systems must technically enforce password complexity, expiration, and reuse controls where feasible.

8. Clean Desk and Computer Use

This policy ensures information remains secure when workstations are unattended and promotes responsible device use, including for remote and hybrid work.

8.1 Clean Desk Standards

- Do not leave confidential papers or devices unattended.
- Lock documents in drawers or cabinets when unsupervised.
- Dispose of sensitive materials using approved shredding or confidential bins.
- Retrieve printouts immediately from printers.
- Keep file cabinets locked.
- Store access cards and keys securely.
- Never record passwords on paper or visible notes.
- Erase whiteboards and clear meeting notes after use.
- Promote a **paper-light** workplace and store files electronically whenever possible.

8.2 Computer Use

- Respect others' privacy; do not view colleagues' screens.
- Lock or log off your computer when leaving your desk.
- Follow the Password Policy.
- Shut down computers properly at day-end.
- Delete obsolete files and maintain organized folders.
- Do not duplicate or delete others' files without authorization.
- Access only data and systems for which authorization is granted.
- Do not use Company systems for personal profit or fraudulent activity.

9. Portable Media and Equipment

Laptops, tablets, and mobile devices are essential tools but also significant risk vectors due to portability and remote use. This policy applies to all Company-issued or personal devices used to access Company data.

9.1 Key Requirements

- Keep devices under direct supervision; lock or log off when unattended.
- Secure devices with passwords, PINs, or biometrics compliant with the Password Policy.
- Keep credentials confidential and never share them.
- Do not lend Company devices to others.
- Store equipment out of sight when not in use; never leave it visible in vehicles.
- Use protective cases to prevent damage.
- Be vigilant in public spaces.
- Encrypt stored files and use full-disk encryption where available.
- Back up data daily to Company servers or approved encrypted media.
- Ensure antivirus protection is active and current.
- Report any loss, theft, or malware infection immediately to management or IT Support.

10. Destruction of Media and Equipment

10.1 Media Disposal

- Shred expired paper records or removable media (CDs, DVDs).
- Securely wipe or degauss drives, USBs, and other storage devices before disposal or reuse.
- Backup tapes must be fully erased and degaussed.
- No media may be destroyed without prior authorization from the CTO or Compliance Officer.

10.2 Equipment Disposal

Only authorized personnel may decommission equipment. Before removal from the network, drives must be wiped or degaussed. Detailed disposal logs must record serial numbers, dates, and responsible staff.

11. Anti-Virus Protection

Antivirus and anti-malware controls protect systems against viruses, Trojans, worms, spyware, and related threats.

11.1 Implementation

- All servers and endpoints must run licensed, approved antivirus software.
- Definitions must update automatically at least once daily.
- Full system scans must run weekly.
- Email attachments and external media must be scanned automatically.
- Users may not disable antivirus protection or updates.
- If malware cannot be cleaned, isolate the system and notify IT Support immediately.

12. Intrusion Prevention

The Company depends on secure, uninterrupted system operation. Both physical and logical intrusion-prevention measures are mandatory.

12.1 Physical Security

- All live production systems are hosted in an **ISO/IEC 27001-certified** data center with controlled access and continuous monitoring.

12.2 Logical Security

- Firewalls must restrict traffic to required ports and services only.
- Only encrypted connections (VPN, TLS 1.2 or higher) may reach production environments.
- Strong passwords and MFA are required for privileged accounts.

- Operating systems and applications must be hardened and patched promptly.
- Antivirus protection must be active on all production and remote-access machines.
- All configuration changes must follow formal change-management procedures.
- Hosting providers must meet industry security standards.

13. Training and Awareness

13.1 Purpose

Training ensures all employees understand their information-security responsibilities and can act to protect Company data.

13.2 Scope

- Mandatory induction training for all new staff.
- Annual refresher training for all personnel.
- Specialized sessions for high-risk or technical roles.

13.3 Content

Covers:

- Core information-security principles and acceptable-use rules.
- Identifying phishing, social-engineering, and malware threats.
- GDPR data-protection obligations.
- Incident-reporting procedures and escalation paths.
- Business-continuity and disaster-recovery awareness.

13.4 Incident Response

Employees must recognize and immediately report suspected breaches to their manager or the Incident-Response Team. Simulated exercises may test readiness.

13.5 Continuous Improvement

Training materials are reviewed annually to incorporate regulatory and technological changes.

Attendance records are maintained to demonstrate compliance with **ISO 27001 Clauses 7.2 and 7.3**.