2026

EULMAN Information Security Charter

Information Security, Confidentiality & Data Protection

Document reference: ELMN-002
Revision: 00
Classification: Public
Approved by: Board of EULMAN SAS
Approval date: 26-06-2026

1. Purpose

Information is a critical asset in EULMAN's activities.

Clients, partners and stakeholders entrust EULMAN with business information, project documentation, personal data, commercial information and, in certain assignments, confidential or sensitive material.

EULMAN is committed to protecting this information throughout its lifecycle.

This Information Security Charter establishes the principles governing the protection, use, storage, transmission and management of information across EULMAN's activities.

Its objectives are to:

- preserve the **confidentiality** of information and prevent unauthorised disclosure;
- maintain the **integrity** and reliability of information and documents;
- ensure appropriate **availability** of information required for business activities;
- apply security measures proportionate to identified risks;
- protect information entrusted by clients, partners and other stakeholders;
- support compliance with applicable legal, regulatory and contractual requirements;
- strengthen organisational resilience and business continuity;
- continuously improve EULMAN's information-security practices.

These principles apply to information regardless of whether it is created, received, processed or stored in electronic, physical or other form.

They apply across EULMAN's activities and, where relevant, to external professionals, service providers and partners who access information under EULMAN's responsibility.

2. Information Security Principles

Confidentiality

Information is made available only to persons who have a legitimate professional need to access it.

Access, sharing and disclosure are determined according to the nature and sensitivity of the information concerned and any applicable contractual, legal or professional requirements.

Integrity

Information should remain accurate, complete and protected against unauthorised or unintended alteration.

Appropriate measures are applied to preserve document integrity, identify relevant versions and reduce the risk of accidental modification, deletion or corruption.

Availability

Information necessary for business activities should remain accessible to authorised users when reasonably required.

EULMAN applies proportionate measures intended to reduce the risk of loss of access resulting from technical incidents, human error or other disruptions.

Need-to-know and least privilege

Access to information and systems is provided according to professional responsibilities and legitimate business needs.

Privileges should be limited to those necessary for the relevant activity and reviewed or withdrawn when no longer required.

Security by design and by default

Information-security considerations should be integrated into the organisation of activities, systems and projects rather than addressed only after implementation.

Where new systems, processes or working methods are introduced, security and data-protection implications are considered according to their nature and associated risks.

Proportionality and risk

Security controls are applied according to the sensitivity of the information, the operating context and the potential consequences of compromise.

Not all information requires identical protection. EULMAN therefore applies a risk-based approach intended to concentrate controls where they are most relevant.

3. Information Classification

EULMAN uses information classification as a fundamental element of its information-security framework.

Information may be classified according to four levels:

PUBLIC

Information approved for public disclosure or whose disclosure does not create a material risk for EULMAN, its clients, partners or stakeholders.

Examples may include published corporate information, public reports, marketing materials and information already lawfully available to the public.

INTERNAL

Information intended primarily for internal professional use whose unauthorised disclosure would not normally result in significant harm, but which is not intended for unrestricted public distribution.

CONFIDENTIAL

Information requiring controlled access because unauthorised disclosure, alteration or loss could adversely affect EULMAN, a client, partner or other stakeholder.

This may include commercial information, proposals, contracts, client documentation, project information, financial information and non-public business material.

RESTRICTED

Information requiring the highest level of protection within EULMAN because unauthorised access, disclosure, alteration or loss could have significant legal, contractual, financial, security or reputational consequences.

Access to Restricted information is limited to specifically authorised persons with a demonstrated professional need.

Classification may determine the appropriate requirements for access, storage, transmission, sharing, retention and disposal.

Where information is provided by a client or third party under specific confidentiality or security requirements, those requirements are taken into consideration in addition to EULMAN's internal classification.

4. Identity and Access Management

Access to EULMAN's information resources is based on identifiable and authorised users.

EULMAN applies access-management principles intended to ensure that:

- access is linked to legitimate professional requirements;
- individual accounts are used wherever reasonably practicable;
- authentication mechanisms are appropriate to the risk associated with the system or information;
- multi-factor authentication is used for relevant services and systems where supported and appropriate;
- administrative or elevated privileges are restricted;
- access rights are adapted when responsibilities change;
- access is withdrawn when no longer justified;
- credentials must not be improperly shared or disclosed.

Access to sensitive information is restricted according to classification, contractual obligations and professional need.

5. Information Handling and Document Control

Information must be handled in a manner appropriate to its classification and purpose.

EULMAN maintains principles for controlled document management intended to support:

- identification of relevant documents;
- appropriate version management;
- distinction between working, reviewed and final information where relevant;
- preservation of document integrity;
- controlled storage;
- appropriate access permissions;
- traceability of significant documents and changes where required;
- secure sharing with authorised recipients;
- prevention of unintended disclosure.

Before information is transmitted externally, consideration should be given to its recipient, classification, transmission method and any applicable confidentiality requirements.

Particular care is applied when information is shared outside EULMAN's controlled environment.

6. Systems, Devices and Cloud Services

EULMAN relies on digital systems and cloud services to perform its professional activities.

Systems used for business information should be selected and configured with appropriate consideration of security, reliability, access control and data protection.

Relevant security practices may include:

- authentication and access controls;
- multi-factor authentication;
- security updates and patching;
- endpoint protection;
- device access protection;
- encryption capabilities where appropriate;
- controlled installation and use of applications;
- backup and recovery mechanisms;
- secure cloud storage and collaboration environments;
- monitoring of relevant security events where appropriate.

Professional information should be processed and stored through authorised systems appropriate to its sensitivity whenever reasonably practicable.

Loss, theft or suspected compromise of a device containing or providing access to EULMAN information must be treated as a potential security incident.

7. Remote and Mobile Working

EULMAN's activities may involve international, remote and mobile working environments.

Information-security requirements therefore apply regardless of physical working location.

Personnel and authorised contributors are expected to take reasonable precautions against:

- unauthorised observation or access;
- loss or theft of devices;

- insecure storage of documents;
- inappropriate use of shared or public equipment;
- unintended disclosure during calls or meetings;
- insecure transmission of sensitive information.

Additional safeguards may be applied where the environment or information concerned presents increased risk.

8. Client and Third-Party Information

Information entrusted to EULMAN by clients and partners is handled according to the same fundamental security principles applied to EULMAN's own information, together with any additional contractual or legal requirements.

Client information is used only for legitimate professional purposes connected with the relevant activity unless otherwise authorised.

EULMAN recognises that external service providers, professionals and partners can introduce information-security dependencies.

Where third parties may access or process relevant information, appropriate consideration is given to:

- the nature and sensitivity of information concerned;
- the purpose and extent of access;
- confidentiality obligations;
- security capabilities;
- applicable data-protection requirements;
- contractual responsibilities;
- access termination when the relationship or requirement ends.

Third-party involvement does not remove EULMAN's responsibility to apply appropriate care to information under its control.

9. Data Protection and Privacy

EULMAN is committed to the responsible processing of personal data.

Personal data is processed according to applicable legal and regulatory requirements, including, where applicable, **Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR)**.

EULMAN's approach reflects fundamental data-protection principles including:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality;
- accountability.

Access to personal data is limited according to legitimate professional requirements.

Where activities, technologies or processing operations may create increased privacy risks, data-protection considerations should be incorporated into their design and implementation.

Information security and data protection are treated as complementary responsibilities.

10. Confidentiality and Professional Discretion

Confidentiality forms part of EULMAN's professional responsibilities.

Information obtained through client assignments, partnerships, negotiations or other professional relationships must not be disclosed or used outside its legitimate purpose without appropriate authorisation or legal basis.

This obligation applies irrespective of the medium in which the information is communicated.

Where appropriate, contractual confidentiality arrangements may supplement EULMAN's internal requirements.

Professional discretion is expected even where information does not formally meet the threshold for Confidential or Restricted classification.

11. Information Security Risk Management

EULMAN applies a risk-based approach to information security.

Information-security risks may arise from technological, organisational, human, physical or third-party factors.

Relevant risks may include:

- unauthorised disclosure;
- loss or theft of information;
- account or credential compromise;
- phishing and social engineering;
- malware or other malicious activity;
- accidental deletion or alteration;
- inappropriate access;
- system or service unavailability;
- third-party compromise;
- loss or theft of devices;
- incorrect transmission of information;
- insufficient backup or recovery capability;
- legal or contractual non-compliance.

Risks are considered according to their likelihood, potential impact and the sensitivity of affected information or activities.

Controls are selected and implemented proportionately.

Information-security risks may be reassessed when material changes occur in systems, activities, suppliers, threats or operating circumstances.

12. Information Security Incidents

Actual or suspected information-security events should be identified, reported and addressed without unnecessary delay.

Relevant events may include suspected unauthorised access, loss of information, compromised credentials, malicious communications, unintended disclosure, device loss or other circumstances capable of affecting confidentiality, integrity or availability.

Depending on the nature of the event, incident management may include:

1. identification and reporting;
2. initial assessment;
3. containment;
4. protection of affected information or systems;
5. investigation and impact assessment;
6. recovery and restoration;
7. communication or notification where required;
8. documentation of relevant findings;
9. corrective action and lessons learned.

Where an incident may constitute a personal-data breach, applicable data-protection requirements and notification obligations are assessed.

Security incidents are also considered opportunities to improve controls and reduce recurrence.

13. Backup, Recovery and Business Continuity

EULMAN seeks to maintain the availability and recoverability of information necessary for its activities.

Proportionate measures may include:

- backup of relevant information;
- use of resilient cloud services;
- appropriate redundancy;
- recovery capabilities;
- preservation of critical documentation;
- alternative communication or access arrangements;
- management of critical service dependencies.

Business continuity and information security are treated as interconnected disciplines.

Recovery priorities are determined according to the importance of affected information, systems and business activities.

14. Information Retention and Secure Disposal

Information should not be retained indefinitely without a legitimate business, contractual or legal reason.

Retention takes into consideration:

- legal requirements;
- contractual obligations;
- business requirements;
- client requirements;
- potential audit or evidence needs;
- data-protection principles;
- information classification.

When information is no longer required and retention is not otherwise justified, it should be deleted, destroyed or otherwise disposed of using methods appropriate to its sensitivity and medium.

Access rights should similarly be removed when their underlying business purpose ends.

15. Security Awareness and Human Responsibility

Technology alone cannot ensure information security.

Every person with access to EULMAN information or systems has a responsibility to exercise appropriate professional care.

This includes awareness of risks such as phishing, credential theft, social engineering, accidental disclosure and inappropriate information sharing.

EULMAN promotes awareness of information-security responsibilities and adapts guidance or controls when changes in activities, technology or threats make this appropriate.

Suspected weaknesses or security events should be reported rather than ignored.

16. Continuous Improvement

Information security is a continuing process.

EULMAN periodically reviews its practices in light of:

- changes in activities and organisational requirements;
- technological developments;
- emerging threats and vulnerabilities;
- security incidents and identified weaknesses;
- client and contractual requirements;
- regulatory developments;
- changes in recognised standards and good practices;
- experience gained through projects and operations.

Where weaknesses or opportunities for improvement are identified, appropriate corrective or improvement measures may be implemented.

The objective is to maintain an information-security framework proportionate to EULMAN's evolving activities and risk environment.

17. Reference Framework

EULMAN's information-security approach is informed by internationally recognised standards, regulatory requirements and professional good practices.

In particular, the framework reflected in this Charter takes into consideration principles addressed by:

ISO/IEC 27001, Information security management systems, particularly the establishment, maintenance and continual improvement of a risk-based Information Security Management System.

ISO/IEC 27002, Information security controls, particularly organisational, people, physical and technological security measures.

ISO/IEC 27005, Information security risk management, particularly the identification, assessment and treatment of information-security risks.

ISO/IEC 27701, Privacy information management, particularly the integration of privacy considerations into information-management practices.

ISO 22301, Business continuity management systems, particularly organisational resilience and continuity of critical activities.

ISO 31000, Risk management, particularly the integration of risk considerations into governance and decision-making.

ISO 9001, Quality management systems, particularly controlled processes, documented information, accountability and continual improvement.

EULMAN also takes into consideration applicable legal, regulatory and contractual requirements, including the **General Data Protection Regulation (EU) 2016/679**, where applicable.

These frameworks provide recognised principles and good practices that inform EULMAN's approach. Their application is proportionate to the organisation's activities, information assets, operating environment and identified risks.

18. Governance of this Charter

This Charter forms part of EULMAN's broader governance framework and applies across the organisation's activities.

Its principles may be implemented through supporting policies, procedures, technical controls, contractual provisions and operational practices.

These may include, where appropriate:

- information-classification rules;
- access-control practices;
- document-management requirements;
- incident-response procedures;
- backup and recovery arrangements;

- business-continuity measures;
- third-party security requirements;
- data-protection procedures.

Detailed internal security controls and procedures are not necessarily made public, as their confidentiality may itself contribute to the protection of EULMAN's information environment.

This Charter is reviewed periodically and when significant organisational, technological, regulatory or risk-related changes make review appropriate.

This Charter should be read in conjunction with the EULMAN Quality Charter (ELMN-001) and other applicable corporate policies and procedures.

Our Commitment

EULMAN recognises that clients and partners must be able to entrust information to us with confidence.

Information security is therefore not treated solely as a technical responsibility. It is integrated into professional conduct, project delivery, document management, risk management and corporate governance.

Our commitment is to protect information through **proportionate controls, responsible behaviour, appropriate technology and continuous improvement**, while enabling the effective delivery of our professional services.

Approved by the Board on 26-06-2026

EULMAN SAS