FEDRIGONI

Information Security Policy

Ver.	Date	Change Description	Author
1.0	15.10.2021	First release	Group IT Security Manager

Issued by	Verified by	Approved by
Group IT Security Manager	Group Chief Information Officer, Group Compliance Officer & Chief Internal Auditor	Group Board of Directors

FEDRIGONI
Group

Sede legale
Via Enrico Fermi 13/f
37135 Verona (VR), Italy
T +39 045 8087888
F +39 045 8009015

Sede operativa
Piazzale Lodi 3
20137 Milano, Italy
T +39 02 467101

fedrigoni.com

1888

FEDRIGONI

Index

FEDRIGONI Group

Sede legale
Via Enrico Fermi 13/f
37135 Verona (VR), Italy
T +39 045 8087888
F +39 045 8009015

Sede operativa
Piazzale Lodi 3
20137 Milano, Italy
T +39 02 467101

fedrigoni.com

1888

1. Policy overview

1.1. Introduction

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.
This document addresses the information security management in Fedrigoni Group to assure adequate security levels for information stored and transmitted using ICT technologies (personal data, financial data, etc...), compliance with regulatory requirements and an effective risk management.
The document is structured in four chapters:

- this Chapter ("Policy Overview") establishes the scope of policy, applicable external and internal references, terms and definitions;
- Chapter 2 ("information Security Policies") describes information security domains to address with security policies;
- Chapter 3 ("Exceptions") defines exceptions to this document;
- Chapter 4 ("Amendment") defines upgrade rules to the document.

1.2. Scope

The purpose of this document is to provide a description of information security policies to adopt within Fedrigoni Group to guarantee an adequate level of information protection in terms of:

- Confidentiality, ensuring that the information is available only to authorized users;
- Integrity, safeguarding the completeness, accuracy and conformity of information during acquisition, storage, processing and presentation;
- Availability, ensuring that authorized users can have access to the information they need for their operations.

Information security policies has been defined in accordance with the international standards (e.g. ISO/IEC 27001) with the regulations regarding information security management practices, organization's information security risk environment and business requirements as well. This document applies to all Legal Entities of Fedrigoni Group.

1.3. References

External references:

- Information technology - Security techniques - Information security management systems [ISO/IEC 27001]
- Information security, cybersecurity and privacy protection - Information security controls [ISO/IEC 27002]
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data [General Data Protection Regulation or GDPR]

1.4. Terms and definitions

For the purposes of this document, following are reported terms and definitions.

Terms	Definitions
Access control	Means to ensure that physical and logical access to assets is authorized and restricted based on business and security requirements
Asset	Anything that has value to the organization
Attack	Unauthorized attempt to destroy, expose, alter or any attempt to disable, steal, gain access to or make unauthorized use of an asset
Authentication	Provision of assurance that a claimed characteristic of an entity is correct
Authorized user	Interested party having formal permission to access information
Business Unit	Part of a Legal Entity that operates as a separate part of the whole business
Control	Measure that maintains and/or modifies risk
Disaster recovery	The set of technological and organizational measures designed to restore systems, data and infrastructures after the occurrence of an event that interrupts business processes
Information	Set of interrelated data that has value for the organization
Information security event	Occurrence indicating a possible breach of information security or failure of controls
Information security incident	One or multiple related and identified information security events that can harm an organization’s assets or compromise its operations
Information security incident management	Exercise of a consistent and effective approach to the handling of information security incidents
Information system	Set of applications, services, information technology assets, or other information-handling components
Legal Entity	Organization that has legal rights and responsibilities

Terms	Definitions
Personally identifiable information (PII)	Any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person
Policy	Intentions and direction of an organization, as formally expressed by its top management
Procedure	Specified way to carry out an activity or a process
Process	Set of interrelated or interacting activities that transforms inputs into outputs
Rule	Accepted principle or instruction that states the organization's expectations on what shall be done, what is allowed or not allowed
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organization
User	Interested party with access to the organization´s information systems

2. Information Security Policies

Fedrigoni Group has defined the security domains to cover with appropriate Group information security policies that all Legal Entities must implement and follow.
Information security domains are categorized into four areas (Organizational, People, Physical and Technological) and are described in the following paragraphs.

- Organizational controls
  - Information security roles and responsibilities
  - Asset management
  - Information classification
  - Access control
  - Third party information security risk
  - Compliance
- People controls
  - Human resources security
- Physical controls
  - Physical security
  - Environmental security
- Technological controls
  - Operations security
  - Communications security
  - Information systems acquisition, development, maintenance and decommissioning
  - Information security incident management
  - Business continuity management and disaster recovery

2.1. Organizational Controls

2.1.1. Information security roles and responsibilities

At Group level, roles and responsibilities regarding information security and related risks management are as follows.

- Group IT Security Manager:
  - Manages information security risk throughout the data lifecycle, for the whole Fedrigoni Group, ensuring the execution of periodical risk assessments to identify priorities for managing information security risks and for implementing controls to reduce these risks;
  - Briefs the executive team on status and cybersecurity risks, including taking the role of champion for the overall strategy and necessary budget;
  - Manages/oversees a staff of information security employees;
  - Coordinates with Compliance Office in order to identify Group regulatory requirements;
  - Sets the information security policies at Group level (strategic focus, group policies and issues of regulatory guidelines);
  - Keeps Group information security procedures up to date;
  - Supports Internal Audit team in performing information security audits;
  - Acts as demand manager against Business to define/evaluate information security requirements in case of new implementations or review of existent;
  - Ensures, through periodical assessments, the effectiveness of information security measures in order to protect company assets and guarantee compliance with the regulations regarding information security management practices and business requirements;
  - Performs information security audit activities on third parties;
  - Supports information security audit activities required by a third party;
  - Manages the design of appropriate information security solutions;
  - Manages the information security incident detection and response activities.
- Group Head of IT Infrastructure, Group Head of Business Intelligence & Digital IT, IT Director BU Self-Adhesives, IT Director BU Paper:
  - Align information technologies with the Group´s information security strategy;
  - Implement the information security solutions designed by the Group IT Security Manager;
  - Facilitate and support periodical security assessments;
  - Implement remediation initiatives identified in information security assessments;
  - Support information security incident detection and response;
  - Manage the information security incident recovery;
  - Perform technical activities to maintain up-to-date IT technical assets.
- Group Compliance Officer & Chief Internal Auditor:
  - Ensures the necessary interpretative support for competence activities on regulatory and legal aspects of information security;
  - Provide advises, inputs and participates the review of IT security policies and regulations;

- Determines the audit activities to be carried out to verify information security management with respect to Group Policies and Procedures;
- Ensures that audit reports and issues related to information security are shared and reported to Group IT Security Manager.

2.1.2. Group Information Security Committee

This policy establishes the Group Information Security Committee. The objective of the Committee is to lead and develop Information Security Initiatives at group level. To fulfil its responsibility the Committee:

- Defines and develop projects to enhance information security across the Group;
- Reviews and approves Group's information security strategy and overall responsibilities;
- Agrees on specific roles and responsibilities for information security across the Group;
- Establishes methodologies and processes for assessing risk and protecting Fedrigoni Group information;
- Ensures that security is part of the information planning and IT process.

The Committee's composed by the following participants:

- Group Chief Information Officer,
- Group IT Security Manager,
- Group Compliance Officer & Chief Internal Auditor,
- Group Human Resources Officer represented by Group Head of Talent Acquisition & Development,
- Group Chief Financial Officer represented by Group Treasury and Risk Director.

The Committee should meet at least quarterly.

Each Business Unit/Legal Entity, if needed, must define and detail internal roles and responsibilities to manage adequately information security topics in coordination with related Group roles. This is particularly significant for Business Unit/Legal Entity where IT adoption is relevant on major business process.

2.1.3. Asset management

All technological assets (hardware[1], software[2] and network[3] assets) associated with Fedrigoni Group's information shall be identified and recorded in an updated inventory.
Asset inventory shall report at least:

- Owner responsible for inventory, classification and protection of asset;

[1] Data processing equipment, transportable equipment, fixed equipment, processing peripherals, data medium, electronic medium, other medium.

[2] Operating system, service software, maintenance software, administration software, package software, standard software, business application

[3] Communications and telecommunications media and equipment, network devices, communication interfaces.

- Classification of information related to asset.

Rules for the acceptable use of assets shall be identified and documented in order to ensure their proper and safe functioning and to reduce and prevent risks (including virus attacks, compromise of network systems and services, legal issues) related to inappropriate use (e.g. human errors, theft, fraud or misuse).
Employees and external party users using or having access to Fedrigoni Group's assets shall be made aware of security requirements of the organization's assets associated with information and shall be responsible for their use of any information processing resources and of any such use carried out under their responsibility.
All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

2.1.4. Information classification

Fedrigoni Group's information shall be classified and labelled in terms of its value, legal requirements, sensitivity and criticality. In addition to common type of data (personally identifiable information, financial data, etc.) industry specific data (e.g. sales network, supply chain management, concessions and acquisitions) shall be evaluated. All data shall have an owner responsible for information classification.
Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by Fedrigoni Group.

2.1.5. Access control

Information shall be protected from unauthorized access to ensure confidentiality, integrity and availability.
The entire life cycle of user access (user account creation, user account change and user account removal) shall be defined to reduce the risk of unauthorized access to information. Moreover, specific requirements shall be defined about password strength and other authentication techniques.
Remote access shall be limited to authorized personnel and performed through encrypted channels using an appropriate MFA (Multi-Factors Authentication) process.
Access profiles shall be coherent with the task being performed (need to know principle) and shall follow a documented approval process. Allocation of privileged access rights (e.g. System Administrator) shall be controlled through a formal authorization process in accordance with access control policy defined.
Periodical review activities of user access privileges shall be performed for all the information systems in order to ensure they are assigned on a "need to know" base. Authorizations for privileged access rights shall be reviewed at more frequent intervals, in relation to the criticality of the systems accessed.

Segregation of duties criteria shall be defined for every process in which data (e.g. financial data, business data, personally identifiable information, etc.) are handled, in order to avoid fraud and misuse.

2.1.6. Third party Information security risk

In case of third parties accessing Fedrigoni Group's information, adequate security measures shall be established to ensure confidentiality, integrity and availability of information.
A third-party information security risk management process shall be defined in order to attribute a risk profile to third parties and identify related security measures to be contracted with them.
Agreements with third parties shall include requirements regarding protection of Fedrigoni Group's data. In particular, third parties shall be available to present, upon request, their security plans and security measures implemented and allow security audits by Fedrigoni Group.
Service Level Agreement (SLA) shall be included in contracts with third parties to punctually define the service levels. Services provided by third parties shall be periodically monitored.

2.1.7. Compliance

Information system management adopted in Fedrigoni Group, shall be compliant with laws (e.g. GDPR), standards and Group policies to prevent risks of no compliance and related consequences (e.g. fines, damage to reputation, contractual penalties, etc.).
As legislative requirements could vary from country to country, it is necessary to implement a compliance management process in order to be able to show compliance with current applicable legislation and to be prepared to timely identify local requirements to maintain the compliance status.
Each Legal Entity shall identify an owner for compliance management process responsible to address, in coordination with the Group IT Security Manager and in coordination with the Group Compliance Officer & Chief Internal Auditor, the activities related to local information security requirements.

2.2. People controls

2.2.1. Human resources security

During hiring activities, verification carried out by the HR department on candidates shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
The contractual agreements with employees and contractors shall state their responsibilities for information security.
Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of Fedrigoni Group. Employees and contractors shall

be aware about security threats and trained on the proper usage of information systems and devices property of Fedrigoni Group (security awareness, education and training).
Employees and contractors shall be aware their information security responsibilities and duties remain valid after termination or change of employment.
The access rights of all employees and contractors to information and information processing facilities shall be removed upon termination of their employment or adjusted upon change.

2.3. Physical controls

2.3.1. Physical security

Physical access controls shall be defined to ensure that only authorized personnel are allowed to access to company areas. In particular, physical security controls shall be enforced where assets processing sensitive or critical business information are maintained. Implementation of security measures shall be addressed according to Fedrigoni Group specific physical layers.
Physical access controls shall be regular monitored to guarantee their effectiveness in protecting against unauthorized accesses.

2.3.2. Environmental security

Equipment shall be protected from environmental threats as well (e.g. fire, flood, electrical supply interference, etc.). A secure working environment shall be established and maintained in line with the current Group policies on Health & Safety.

2.4. Technological controls

2.4.1. Operations security

Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled and documented (change management).
The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance (capacity management) taking into account the business criticality of the concerned systems.
Fedrigoni Group information back-up shall be taken and tested regularly to maintain the availability of data, in line with associated risks. Moreover, software and information processing facilities shall be protected from malicious code to ensure the integrity of software and information.
Event logs recording user, system administrator and system operator activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. Logging activities shall be carried out in compliance with current legislation.

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
Each Legal Entity, taking into consideration its business contest and related risks, shall evaluate the implementation of data masking procedure (e.g. to protect personally identifiable information) and data leakage prevention systems or techniques in order to identity, monitor e protect information from unauthorized access.

2.4.2. Communications security

Communication and network devices shall be protected to ensure data integrity, confidentiality and availability. Network devices security shall be properly configured, to assure the right segregation between different purpose environments. Security regarding data exchange among different location (plants, headquarters and warehouses) and third parties shall be addressed as well by means of security measures (e.g. data encryption).

2.4.3. Information systems acquisition, development, maintenance and decommissioning

A clear system development life cycle and its phases (installation, configuration, maintenance and decommissioning) shall be defined to prevent data loss or unauthorized modification. Development, testing and production environment shall be segregated and access to program source code shall be restricted.
Group policies shall be defined to evaluate security measures related to the adoption of cloud services and mobile computing devices.
In order to identify agree on security requirements prior to the development and/or implementation of information systems, a security by design process shall be defined and implemented at Group level.

2.4.4. Information security incident management

Information security events and weaknesses associated with information systems shall be communicated timely to take corrective actions.
Event reporting and escalation procedures shall be in place. All employees and users shall be made aware of how they could report the different types of event that might have an impact on the security of Fedrigoni Group’s assets.
Managing activities of information security incidents shall be aligned with the process defined at Group level. In case of PII data breach, managing activities shall be compliant with current regulatory requirements (e.g. GDPR).

2.4.5. Business Continuity management

A Business Continuity management system is a set of processes, procedures and technological systems aimed at guaranteeing the continuity of business activities, in the event of significant events/disasters, minimizing the related impacts (e.g. loss of revenues, loss of operational efficiency, loss of image and reputation, etc.). To establish a Business Continuity management system shall be analysed the business context of Fedrigoni Group, defined the related business continuity strategies (Business Continuity plan) and technological and organizational measures to restore systems, data and infrastructures after the occurrence of an event that interrupts business processes (Disaster Recovery plan).
Business Continuity plan and the Disaster Recovery plan shall be regularly tested in order to verify their effectiveness and efficiency and reviewed and updated periodically in case of significant changes in Group's context.

3. Exceptions

Legal Entities or Business Units may decide to be more restrictive on any of the requirements. These are not considered exceptions to the Policy therefore just need to be notified to the Group IT Security Manager.
Exceptions to this Policy must be formally approved by the Group IT Security Manager in accordance with the Fedrigoni Group guiding principles.

4. Amendment

This Policy must be formally reviewed at least once every three years.
Changes that due to their importance cannot wait until the end of the three-year period must be dealt in coordination with the Group Compliance Officer and Chief Internal Auditor.