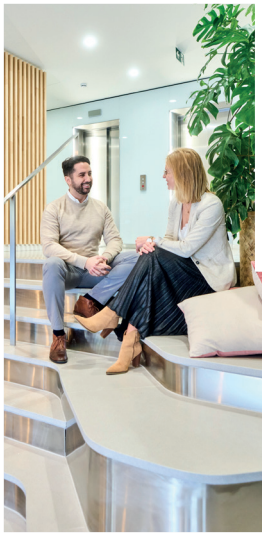
Cofinimmo

together in real estate

CYBERSECURITY POLICY



Document finalised on 18.12.2025

Last update on 15.12.2025

Originally written in English

CYBERSECURITY POLICY

CONTENT

I. AUTHORITY, DISTRIBUTION AND REVIEW

1 Distribution and accessibility

This document is publicly accessible and distributed to all relevant stakeholders.

2 Review and maintenance

This policy, along with all supporting documents and procedures, will be reviewed annually or whenever significant changes occur in organisational structure, technology, or regulatory requirements. Updates and improvements will be made to ensure ongoing alignment with best practice and legal requirements.

II. PURPOSE AND SCOPE

1 Purpose

The Organisation (see section 4 below) recognises the crucial importance of safeguarding information assets in the pursuit of its business objectives. In an environment where information systems are increasingly interconnected and accessible, the risk of hostile attacks, data loss, or compromise has never been greater. This Cybersecurity Policy establishes the minimum governance requirements for all departments and entities within the Organisation, ensuring the protection of intellectual property, commercial advantage, and our people from the repercussions of poor information security and cyber-attacks.

Due consideration is also given to compliance with laws and regulations.

This policy document is part of a set of policy documents that support the Organisation in establishing a sound cybersecurity strategy.

2 Scope

This policy applies to all information and information systems managed by the Organisation, including but not limited to:

- Information systems and assets provided or maintained by the Organisation;
- Internal and external individuals processing organisational information;
- All devices and endpoints used for information processing;
- Procedures and processes supporting information management;
- Physical and virtual locations where organisational activities are conducted;
- Any other elements that may present a cybersecurity risk.

Critical and confidential information or systems are those whose confidentiality, integrity, or availability, if compromised, would significantly harm the Organisation.

"In an environment where information systems are increasingly interconnected and accessible, the risk of hostile attacks, data loss, or compromise has never been greater.

III. DEFINITIONS

Specific terms and abbreviations used in this document are defined here.

Term	Description
The Organisation	All Cofinimmo Group companies and subsidiaries
Information Security Manager	Head of IT or appointed equivalent (supportit@cofinimmo.be)
Subcontractors	External individuals or entities engaged by the Organisation who process organisational information or have access to information systems and are required to comply with the same cybersecurity controls, training, and awareness programmes as employees.
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes[1].
Integrity	Property of accuracy and completeness, meaning that data has not been changed, destroyed, or lost in an unauthorized or accidental manner[1].
Availability	Property of being accessible and usable on demand by an authorized entity[1].

IV. POLICY STATEMENTS

1 Governance and responsibilities

Roles and responsibilities for cybersecurity are clearly defined and communicated to all internal and external stakeholders. The Information Security Manager is responsible for maintaining this policy, providing guidance, and ensuring its implementation across the Organisation. Senior Management endorses and supports this policy, with all C-levels and managers accountable for compliance within their respective departments. Regular reviews and updates are conducted at least annually, or more frequently as necessary.

2 Policy principles

- Effective policies and procedures are established and maintained, with clear awareness of information security risks across the Organisation.
- The Organisation maintains an up-to-date inventory of all physical devices, systems, and software, ensuring their ongoing availability and integrity.
- Security controls, such as antivirus and anti-malware solutions, are deployed and maintained on all relevant systems and endpoints.
- The corporate network is protected in accordance with the Network Security Policy, with regular patching and vulnerability management.

1 Source: ISO27000:2018 Overview and Vocabulary (https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip)

- Access management enforces principles of minimum access and multifactor authentication, as detailed in the Access and Password Policies.
- Regular training and awareness programmes are provided to employees and subcontractors, including communication of the Organisation's 10 golden rules for cybersecurity[2].
- Processes are in place for backup, disaster recovery, and incident response, ensuring business continuity and compliance with legal and regulatory obligations.
- All actual or suspected security incidents must be reported immediately to the Information Security Manager for thorough investigation and response.

All policies, procedures, and controls are subject to a process of continual improvement, adapting to changes in the Organisation and its risk environment.

3 Legal and regulatory requirements

The Organisation is committed to identifying, assessing, and implementing all applicable legal and regulatory requirements relating to information and cybersecurity. This process includes maintaining an up-to-date register of relevant laws, statutory obligations, and industry-specific regulations that apply to the handling, storage, and processing of information assets.

Regular assessments are performed to maintain compliance with evolving legal frameworks, such as data protection, privacy, and cybersecurity legislation. The Information Security Manager is tasked with tracking regulatory developments and ensuring that necessary controls, procedures, and documentation are promptly updated in response to new or amended requirements. In relation to GDPR regulations, the privacy team assumes responsibility for monitoring regulatory changes and implementing relevant updates to organizational controls and documentation. When required, the Organisation proactively seeks expert legal counsel to interpret and fulfil complex obligations, guaranteeing that all personnel receive appropriate guidance through targeted training and communications.

"Regular assessments are performed to maintain compliance with evolving legal frameworks, such as data protection, privacy, and cybersecurity legislation.

2 Part of cybersecurity awareness program : comprehensive set of guidelines and best practices aimed at enhancing cybersecurity practices for individuals in the organisation.