GENESIS PROPERTY

CYBERSECURITY POLICY

CYBERSECURITY POLICY

Last update: 29 May 2024

Purpose

This Cyber Security Policy was created to protect the sensitive information, the IT infrastructure at Genesis Property and to ensure the continuity of the operations.

The main objectives of this Cyber Security Policy are the following:

- ***Protection of Sensitive Information***: Ensuring the confidentiality, integrity and availability of critical information
- ***Continuity of Operations***: Ensuring the continuity of IT services by effectively preventing and managing security incidents
- ***Controlled Access***: Limiting access to information and IT resources to authorized persons only
- ***Minimizing Risks***: Implementing preventive and reactive measures to minimize cyber security risks
- ***Legal Compliance***: Ensuring compliance with legal regulations and industry standards

The Cyber Security Policy applies to all employees, regardless of the position held, including temporary employees, contractors and sub-contractors, partners, consultants, all persons representing each company within Genesis Property, as well as any third parties who have access to IT systems and information belonging to Genesis Property.

Responsibilities and Administration

The supervision and support of the Cyber Security Policy falls under the attributions of senior management. The IT department is responsible for the implementation, monitoring and continuous improvement of security measures, and employees shall be committed to complying with IT security policies and procedures.

Classification of Information

Information is classified according to its sensitivity (public, internal, confidential, strictly confidential) and safeguards are adapted and applied according to the classification of the information, including encryption, controlled access and secure storage.

Security of Networks and Systems

Access Control

All devices connected to the network are protected by firewalls, intrusion detection systems and other security measures. Security updates and patches are applied regularly for all systems and applications. Data backups are periodically made and stored in secure locations.

	Access to computer systems is granted on a need-to-know basis. Each user has a unique account and multi-factor authentication for access to critical systems. Unauthorized access is strictly prohibited and immediately revoked in the event of termination of the employment or contractual relationship.
Response to Security Incidents	Any IT security incident shall be reported immediately to the IT department, who will take the necessary steps based on the incident response plan implemented within Genesis Property to manage and remediate security incidents safely, promptly and effectively. Post-incident analysis will be carried out to prevent recurrence and improve security measures.
Training of Employees	All employees participate in regular IT security training sessions, and to promote good security practices within Genesis Property, internal awareness campaigns are conducted periodically.
Monitoring and Auditing	IT security activities are continuously monitored to detect and prevent potential threats. Security audits are regularly conducted to ensure compliance with the IT security policy and to identify areas for improvement.
Implementation and Review	Genesis Property is committed to overseeing the implementation and effective enforcement of the principles of this Cyber Security Policy. The content of this document must be reviewed and updated annually or whenever deemed necessary, based on the results obtained and experience gained and to reflect changes in the IT environment and legal regulations. Any changes to the policy will be communicated to all employees and relevant parties. Failure to comply with the Cyber Security Policy may result in disciplinary sanctions, including termination of employment, in accordance with the internal regulations of Genesis Property companies.