

Cyber & Information Security Policy

Document	Cyber & Information Security Policy
Date	07/08/2026
Revision	v.00
Approval	This Policy has been reviewed and approved by EE Group Leadership Team and is effective as of 07/08/2026

Contents

1	Introduction	2
1.1	Purpose	2
1.2	Scope	2
1.3	Internal Review and Approval	3
1.4	Acronyms	3
2	Security Principles	3
2.1	Cybersecurity principles	3
2.2	Information Security	4
3	Roles and Responsibilities	4
3.1	Group Leadership Team	4
3.2	Information and Communications Systems Security Officer (ICSSO)	4
3.3	Employees	5
4	Acceptable Use	6
5	Access Control	7
6	Access to Premises	7
7	Information Handling & Data Protection	8
8	Device & Endpoint Security	9
9	Network Security	9
10	Third-Party & Cloud Security	10
11	Security Incident Reporting	10
11.1	What constitutes a security incident	11
11.2	Reporting	11
11.3	Response	11
12	Cybersecurity Risk Management	11
13	Vulnerability Management	12
14	Business Continuity & Disaster Recovery	12
15	Monitoring & Compliance	13
15.1	Monitoring	13
15.2	Compliance	13
16	Training & Awareness	13
17	Continuous Improvement	14



1 Introduction

EuroEnergy operates in a digital environment where cyber threats, including malware, ransomware, unauthorized access, data breaches, and social engineering, continue to evolve in complexity. These risks may lead to financial losses, operational disruption, reputational damage, and regulatory penalties. As digital systems, cloud services, and interconnected devices become central to EuroEnergy's operations, safeguarding information assets is essential.

The Group is committed to maintaining a robust cybersecurity posture through proactive risk mitigation, secure IT and OT environments, continuous monitoring, business continuity planning, and timely incident response.

Cybersecurity forms an integral part of the Group's enterprise risk management framework. The Group adopts a risk-based approach to identify, assess, manage, and continuously improve cybersecurity measures, considering evolving threats, regulatory requirements, and the criticality of its energy generation and storage operations.

1.1 Purpose

This Policy defines how EuroEnergy protects its information, systems, and users across the Group. It establishes the principles, responsibilities, and controls required to safeguard EuroEnergy's information assets and digital infrastructure.

The purpose of this Policy is to:

- Protect the confidentiality, integrity, and availability of EuroEnergy information.
- Ensure compliance with applicable laws and regulatory requirements, including GDPR, the NIS2 Directive, applicable national implementing legislation and industry best practices.
- Define acceptable use of EuroEnergy systems, devices, accounts, and data.
- Promote consistent security practices across all EuroEnergy Group companies, employees, contractors, and partners.

1.2 Scope

This Policy applies to:

- All EuroEnergy Group companies, including the parent company and subsidiaries.
- All employees, contractors, partners, and third parties who access EuroEnergy systems or data.
- All EuroEnergy-owned devices, cloud services, network resources, servers, and applications.
- OT environments supporting EuroEnergy's renewable energy assets, including SCADA systems, monitoring and telemetry platforms, energy storage systems, communications infrastructure, and remote access solutions.



All entities must adhere to this Policy to ensure consistent and responsible cybersecurity and information security practices across the Group.

1.3 Internal Review and Approval

This Policy is reviewed by the IT Manager at least annually, or sooner if significant changes occur in the threat landscape, operational environment, technology infrastructure, or regulatory requirements.

Policy updates are submitted to the EuroEnergy Group Leadership Team for final approval.

1.4 Acronyms

Acronym	Description
EE or Group	EuroEnergy Group
ESG	Environmental Social & Governance
ICT	Information & Communication Technology
IT	Information Technology
GDPR	General Data Protection Regulation
OT	Operational Technology
ICSSO	Information and Communication Systems Security Officer

2 Security Principles

2.1 Cybersecurity principles

EuroEnergy operates under these guiding principles:

- Risk-based approach: Cybersecurity risks are identified, assessed, managed, and periodically reviewed as part of the Group's risk management framework.
- Least privilege: Users are granted only the access necessary to perform their roles and responsibilities.
- Defense in depth: Multiple layers of technical, physical, and organizational security controls are implemented to protect systems, networks, and information.
- Secure-by-design and secure-by-default: Security requirements are considered throughout the acquisition, implementation, and operation of technologies, and systems are configured with security controls enabled by default where appropriate.
- Resilience and continuity: Cybersecurity measures support the continued operation and recovery of critical business and operational processes in the event of disruption.
- Continuous improvement: Cybersecurity controls, processes, and practices are regularly reviewed and enhanced to address evolving threats, technologies, and regulatory requirements.



2.2 Information Security

EuroEnergy safeguards information assets by ensuring:

- Confidentiality: Information is accessible only to authorized individuals.
- Integrity: Information is accurate, complete, and protected from unauthorized modification.
- Availability: Systems and data remain accessible to authorized users when required.

Information includes all digital, printed, visual, or verbal information created or managed by EuroEnergy. Information is protected throughout its lifecycle, including creation, storage, processing, transmission, sharing, archiving, and disposal. Appropriate technical and organizational measures are implemented based on the sensitivity and criticality of the information.

3 Roles and Responsibilities

Effective cybersecurity requires clearly defined responsibilities across the Group. The following section outlines these roles and responsibilities.

3.1 Group Leadership Team

The Group Leadership Team is responsible for approving, overseeing and monitoring the implementation of cybersecurity risk management measures and ensuring compliance with applicable cybersecurity obligations. Specifically, the Group Leadership Team:

- Approves this Policy and significant cybersecurity-related policies and procedures.
- Oversee the implementation and effectiveness of cybersecurity risk management measures.
- Reviews significant cybersecurity risks, incidents, and emerging threats periodically.
- Ensures that adequate financial, technological, and human resources are allocated to cybersecurity.
- Promotes a culture of cybersecurity awareness and compliance throughout the organization.
- Supports compliance with applicable legal, regulatory, and contractual cybersecurity requirements. Periodically reviews the effectiveness of cybersecurity controls, compliance obligations and associated risk management measures.

3.2 Information and Communications Systems Security Officer (ICSSO)

The Group IT Manager also serves as the Information and Communications Systems Security Officer (ICSSO) for EuroEnergy Group. The IT Manager/ICSSO is responsible for coordinating the implementation of this Policy, supporting cybersecurity governance and oversight across the Group, reporting cybersecurity matters to the Group Leadership Team, and overseeing the operational IT and information security activities required to achieve the Group's cybersecurity objectives.



In fulfilling these responsibilities, the Group IT Manager / ICSSO performs the following activities:

- Supports the identification, assessment and monitoring of cybersecurity risks.
- Maintains cybersecurity controls and supporting procedures.
- Oversees the implementation and maintenance of cybersecurity safeguards and technologies.
- Provides strategic direction for cybersecurity initiatives across the Group.
- Provides employees with the IT equipment required for the effective performance of their day-to-day work.
- Ensures appropriate allocation of resources for security.
- Monitors network traffic, logs, alerts, and system activity to identify incidents or anomalies.
- Conducts periodic security assessments to evaluate control effectiveness.
- Manages access control processes, including granting, modifying and revoking access.
- Coordinates cybersecurity incident management and response activities.
- Coordinates and supports cybersecurity awareness and training initiatives.
- Coordinates cybersecurity-related assessments, audits, and reviews where applicable.
- Supports employees with IT security guidance and awareness communications.
- Supports compliance with applicable regulatory, ESG-related, and contractual cybersecurity requirements.
- Coordinates cybersecurity regulatory communications and reporting obligations where required by applicable legislation.

3.3 Employees

Employees play a crucial role in EuroEnergy's layered cybersecurity posture, supporting the organization's defenses against cyber threats. Their responsibilities include:

- Complying with this Policy and any related procedures or guidance.
- Keeping passwords confidential, using strong, unique passwords, and enabling multi-factor authentication (MFA) where available.
- Handling EE information responsibly and in accordance with classification rules.
- Being cautious with unsolicited or unexpected (phishing) emails and verifying suspicious requests using known contact details.
- Staying alert to impersonation attempts by e-mail or phone (vishing) and never sharing credentials or confidential information without confirming the sender's or caller's identity.
- Keeping all software, operating systems, browsers, and email applications updated with the latest security patches.
- Avoiding access to sensitive company information over public or unsecured Wi-Fi; using a secure connection such as a mobile hotspot when necessary.



- If unauthorized access to any corporate device is detected, inform the IT Manager immediately to minimize security risks. Using only approved tools and platforms for communication and file sharing.
- Remaining vigilant despite antivirus and firewall protections and always following secure practices.
- Reporting any suspected cybersecurity incidents, suspicious emails, phone calls, unusual system activity, phishing or vishing attempts, malware, loss of devices, unauthorized access, or other security concerns to the IT Manager immediately.
- Reviewing and following periodic security awareness communications issued by the IT Manager.

4 Acceptable Use

All EuroEnergy IT systems, equipment and information are owned by EuroEnergy Group and must be used responsibly and only for legitimate business purposes. The following rules apply under this Policy:

- IT systems are essential to EE Group operations and must be used only for legitimate business purposes by authorized personnel.
- Only approved software, applications and cloud services may be used for business purposes. Employees must not install, copy or delete software without IT Manager approval. If additional software is required for their work, the IT Manager / ICSSO should be advised for approval.
- Passwords must remain confidential and must not be shared.
- Suspicious emails, malware, or other security concerns must be reported immediately to the IT Manager to initiate an appropriate investigation.
- Sensitive data must not be stored on unsecured external media.
- Personal use must not interfere with business operations.
- Employees must not engage in illegal, offensive, or inappropriate activities and communications that violate the Group's policies.
- Employees are responsible for all activity conducted under their user ID.
- EE-issued devices must be secured when unattended, through screen locking or equivalent access controls.
- Employees must not attempt to disable or bypass security controls.
- Business communications must be conducted through approved communication platforms that provide appropriate security controls and protections.



5 Access Control

The following access controls apply across all EuroEnergy IT systems:

User Accounts & Authentication

- All user accounts must be unique and assigned to an identifiable individual.
- Multi-Factor Authentication (MFA) is required for all remote access and for business-critical systems supported by the technology.
- Passwords must meet EE Group security requirements and must be changed immediately if compromised.
- Shared user accounts are prohibited unless specifically approved for operational or technical purposes and subject to appropriate controls.
- User access rights are reviewed periodically to ensure continued appropriateness.

Privileged Access

- Administrative or elevated access is granted only to authorized personnel based on business requirements and approved by the IT Manager. Privileged accounts must not be used for day-to-day work.
- Privileged access rights must be reviewed periodically and removed when no longer required.

Operational Technology Access

- Access to critical OT systems, including SCADA and monitoring platforms, is restricted to authorized personnel and protected through appropriate authentication and access-control mechanisms.
- Remote access to OT systems must be approved by the IT Manager and limited to authorized users and service providers where required for operational purposes and secured through appropriate controls.
- Access rights to OT systems are reviewed periodically and removed when no longer required.

Joiner - Mover - Leaver Process

- Access is granted based on job responsibilities and the principle of least privilege.
- Access is reviewed and updated when job roles change.
- Access is revoked promptly upon termination of employment.
- Access requests and approvals are documented and retained in accordance with applicable procedures.

6 Access to Premises

Access to EuroEnergy premises and areas containing information, OT or communications equipment is controlled to protect personnel, information assets, and systems. Specifically:



- Access cards, keys and access codes must not be shared with unauthorized people.
- Visitors, contractors and other third parties must be accompanied or otherwise appropriately supervised while on EE premises, unless authorized access has been granted.
- Physical access to areas containing critical IT or OT equipment is restricted to authorized personnel.
- Lost or stolen access cards, keys or access credentials must be reported immediately to the IT Manager or the designated responsible person.
- Physical security incidents or suspicious activity affecting EuroEnergy premises, facilities or equipment must be reported promptly.

7 Information Handling & Data Protection

EuroEnergy processes confidential information, including personal data of employees, customers, and partners. All staff must always protect such information.

Data Classification

Information must be classified as Confidential, Internal, or Public. Information owners and users must ensure that information is classified appropriately based on its sensitivity, business value, and legal or regulatory requirements.

Storage & Transfer

- All EE information, including documents, data, records, drafts, and communications created or used in the course of business, must be stored in access-controlled locations with appropriate backup mechanisms enabled where applicable (e.g., secure cloud platforms and company-managed file servers and network drives).
- Access to information is limited to authorized individuals on a need-to-know basis and in accordance with the principle of least privilege.
- Confidential or sensitive information shared or transmitted electronically must be restricted to authorized recipients and protected using appropriate security measures, including encryption where appropriate.
- Sensitive information must not be stored on unencrypted removable media (e.g., USB drives or external hard drives).
- Work emails must not be forwarded or redirected to personal email accounts.
- Personal cloud storage, file-sharing services and collaboration platforms must not be used to store or exchange EE information unless specifically approved.
- Data generated by OT systems, including SCADA, monitoring and telemetry platforms, must be protected against unauthorized access, modification, disclosure or loss.

Physical Information

Employees should always consider whether it is necessary to print documents of a confidential or sensitive nature. Secure printing is enforced through password-protected access.



A clean-desk approach is required at all times:

- Confidential documents must not be left unattended in unsecured areas.
- Hardcopy materials must be securely stored and disposed of using approved methods (e.g., locked storage and secure shredding).
- Confidential information displayed on screens or other devices must not be left unattended or visible to unauthorized people.

Cryptography & Encryption

Appropriate cryptographic controls are implemented to protect sensitive information during storage and transmission. Encryption is applied to mobile devices, portable media, backup data, cloud storage, and electronic communications where appropriate and proportionate to the associated risks.

8 Device & Endpoint Security

EuroEnergy Group devices must be protected through appropriate technical and administrative security controls to reduce the risk of unauthorised access, malware infection, data loss, and compromise of company information.

- EE-managed devices must use approved security controls, including antivirus/anti-malware protection where applicable.
- Operating systems, applications, and security software must be maintained with current security updates and patches, with automatic updates enabled where technically feasible.
- Portable storage devices (e.g., USB drives and external hard drives) must be scanned for malicious content before or upon connection to EE devices.
- Lost or stolen devices must be reported immediately to the IT Manager.
- Devices used to access or store EE information must be protected through appropriate authentication mechanisms, encryption where applicable, and physical security measures.
- Only authorized and approved devices may be used to access EE systems and information.
- Where technically feasible, EE-managed devices should support remote lock and remote wipe capabilities.

9 Network Security

EuroEnergy maintains network security controls appropriate to the risks associated with its operations and assets. Such controls may include firewalls, secure VPN access, intrusion detection and prevention mechanisms, email security filtering, network monitoring, and access control measures.



Users must not bypass, disable or interfere with network security controls.

Network and communications infrastructure supporting critical business and OT systems must be appropriately protected against unauthorized access and cyber threats.

Remote access connections must use secure authentication mechanisms and be restricted to authorized users.

Cyber and information security risks form part of the Group's overall risk management framework and are periodically assessed within EE's enterprise risk register.

Where appropriate, critical OT networks must be logically or physically segregated from corporate IT networks.

10 Third-Party & Cloud Security

- Third-party providers handling EuroEnergy information must adhere to appropriate security and data protection standards.
- Critical ICT suppliers may be subject to proportionate cybersecurity due diligence prior to engagement. Confidential data must not be shared using unauthorized cloud platforms. Cybersecurity risks associated with suppliers, contractors, service providers, and cloud providers must be considered as part of EuroEnergy's risk management processes.
- Contracts with key third-party providers shall include appropriate confidentiality, data protection, information security, and incident notification obligations.
- Third-party access to EE systems must be restricted to authorized users and managed according to business requirements.
- Critical suppliers may be subject to periodic reassessment where appropriate.
- Cloud services used to store or process EE information must be approved by the IT Manager.
- Third-party providers must notify EE without undue delay of cybersecurity incidents that may affect EuroEnergy systems, services or information.

11 Security Incident Reporting

Establishing robust procedures for reporting security incidents, vulnerabilities, and policy violations enables EuroEnergy to effectively identify, assess, and respond to cybersecurity threats. By fostering a culture of transparency and accountability, where employees feel comfortable reporting security concerns without fear of retribution, EE supports the early detection and mitigation of security incidents, thereby strengthening the organization's overall cybersecurity posture.



11.1 What constitutes a security incident

A security incident may include, but is not limited to:

- Malware or ransomware infections.
- Unauthorized access or attempted unauthorized access.
- Loss, theft, or compromise of devices.
- Data loss, data breaches, or accidental disclosure of information.
- Phishing, vishing or other social engineering attempts.
- Disruption to IT or OT systems.
- Compromise of user accounts, passwords or authentication credentials.
- Violations of this Policy or related cybersecurity procedures.

11.2 Reporting

All suspected cybersecurity incidents, vulnerabilities, or security concerns must be reported immediately to the IT Manager. Employees must not investigate incidents themselves unless authorized to do so.

Reports must be made as soon as practicable following detection to support timely containment, investigation and response.

11.3 Response

Upon receipt of a report or notification, the IT Manager will:

- Assess, investigate and contain the incident.
- Escalate significant cybersecurity incidents to relevant management stakeholders as appropriate.
- Coordinate appropriate remediation actions and restoration of affected services where necessary.
- Maintain records of significant incidents and response activities.
- Notify the Group Leadership Team of significant incidents.
- Coordinate internal and external communications where necessary.
- Coordinate regulatory notifications where required by applicable legislation, regulations or contractual obligations (e.g. GDPR or cybersecurity reporting obligations).
- Identify lessons learned and corrective actions following significant incidents.

Significant cybersecurity incidents shall be assessed against applicable regulatory reporting thresholds.

12 Cybersecurity Risk Management

EuroEnergy adopts a risk-based approach to cybersecurity and information security.



- Cybersecurity risks are identified, assessed and managed as part of the Group's enterprise risk management framework.
- Risk assessments may consider threats affecting IT, OT, personnel, suppliers, physical assets and information.
- Significant cyber risks shall be periodically reviewed and communicated to the Group Leadership Team, as appropriate. Appropriate risk treatment measures shall be implemented based on the nature and severity of identified risks.
- Cybersecurity risks shall be reviewed periodically and when significant changes occur in business operations, technology or the threat landscape.
- Significant changes to information systems, operational technology systems, business processes or supplier arrangements may trigger a cybersecurity risk assessment.

13 Vulnerability Management

EuroEnergy takes appropriate measures to identify, assess and address vulnerabilities affecting its systems, applications and devices based on risk and operational requirements. Specifically:

- Security vulnerabilities are evaluated and remediated based on risk and criticality.
- Security patches and updates are applied in a timely manner.
- Vulnerability management activities may include security reviews, assessments, testing and other appropriate measures. Significant vulnerabilities affecting critical systems are prioritized for investigation and remediation.

14 Business Continuity & Disaster Recovery

The Group maintains appropriate arrangements to support the continuity and restoration of critical business and operational activities following a disruption or cybersecurity incident, including and not limited to:

- Critical information and systems are subject to backup and recovery arrangements.
- Backup copies are protected from unauthorized access, modification or loss.
- Recovery capabilities and arrangements are reviewed and tested where appropriate. Business continuity and disaster recovery considerations are incorporated into cybersecurity planning and incident response activities.
- Significant disruptions affecting critical IT or OT systems are managed in a manner that minimizes operational, financial and reputational impacts.



15 Monitoring & Compliance

15.1 Monitoring

EuroEnergy reserves the right to monitor the use of its IT systems and assets, to maintain security and compliance. Specifically:

- Network traffic
- System logs
- Email and internet usage
- Security alerts
- Security incidents and their resolution

Monitoring is conducted to maintain security, detect misuse, and protect EuroEnergy Group assets, in accordance with applicable legal, regulatory, and privacy requirements.

15.2 Compliance

EuroEnergy aims to meet applicable legal, regulatory, and contractual obligations. Compliance efforts may include:

- Implementing controls aligned with applicable legal, regulatory and contractual requirements, including cybersecurity and data protection obligations (e.g. GDPR and ISO-aligned practices).
- Conducting periodic assessments, audits and reviews of cybersecurity controls.
- Addressing identified gaps through corrective actions and continuous improvement activities.
- Maintaining documentation and records to support compliance activities.
- Periodically reviewing the effectiveness of cybersecurity measures and controls.

16 Training & Awareness

EuroEnergy promotes cybersecurity awareness through periodic communications, guidance, and reminders issued by the IT Manager. Employees are required to review and follow these communications.

Additionally, regular updates to training materials ensure that employees remain informed about emerging threats and technologies, enabling them to adapt to evolving cybersecurity risks.

Cybersecurity awareness activities are conducted periodically and may include training sessions, guidance, awareness campaigns, reminders and phishing awareness exercises. EuroEnergy aims to establish and maintain appropriate cybersecurity awareness training programs to support employees in understanding and managing evolving cybersecurity risks. Employees are expected to complete any mandatory cybersecurity training assigned to them.



Members of the Group Leadership Team shall periodically receive appropriate periodic cybersecurity awareness training to enable effective oversight of cybersecurity risk management measures and fulfill applicable regulatory responsibilities.

17 Continuous Improvement

EuroEnergy remains committed to evaluating, refining, and enhancing its cybersecurity measures to adapt to emerging threats, leverage new technologies, and address evolving regulatory requirements. By embracing a philosophy of continuous improvement, EuroEnergy ensures that its cybersecurity posture remains resilient, adaptive, and effective in safeguarding its assets and interests.

