GLOBAL INFORMATION SECURITY & PRIVACY POLICY

1. Objective

This policy expresses the vision of ECO3's management on Information Security & Privacy.

The policy creates a framework for ECO3 to protect through its operations and processes, within reason, all information in scope from any threats, whether internal, external, deliberate or accidental and to mitigate remaining risks towards an acceptable level.

2. Scope

This global Information Security & Privacy **(ISP)** policy is applicable to all organizations belonging to the ECO3 Group and those organizations affiliated with the ECO3 Group and to which ECO3 policies apply irrespective of:

- Site
- Facilities and
- Operations

In the remainder of the text, ECO3 refers to all the above organizations.

This policy covers information and data (hereinafter referred to as "**Data**") that ECO3 handles in its activities, solutions, products and services during their entire lifecycle, as manufacturer, service provider, data controller or data processor.

> Information takes many forms and includes information stored on computers and various other intelligent devices (such as smart phones, tablets, ...), transmitted across networks, printed out or written on paper, sent by fax, stored on tape, disk or usb stick, or spoken in conversation and over the phone.
>
> By handling is meant, without being exhaustive, any operation or set of operations (which is performed on information) whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, irrespective of the media, engines and platforms being used.

This policy applies to all ECO3 staff and to all ECO3 sites, suppliers, contractors and consultants, irrespective of:

- the nature or duration of their work or
- their geographic location

3. Information Security & Privacy Policy

3.1. Information Security and Privacy Objectives

ECO3 is committed to being an organization that secures information and protects privacy of that information, irrespective of whether it is owned by (as data controller) or entrusted to ECO3 (as data processor).

As such, ECO3 strives:

- to make information security & privacy an integral part of the quality of ECO3 solutions, products and services and of its organization and operations;
- to secure information as critical assets of the ECO3 business
- to protect information of partners and customers
- to respect privacy, particularly of employees, partners and customers
- to comply with various privacy and security regulations which are applicable to ECO3 and its various activities
- to create a corresponding awareness, insight and knowledge with ECO3 employees

3.2. Obligations

This policy imposes the following obligations:

- information is protected against unauthorized access;
- confidentiality of information is assured;
- integrity of information is maintained;
- business requirements for the availability of information and information systems are met;
- products and services are secured for our customers
- securing ECO3 core processes
- information is stored only as long as necessary for the fulfillment of the proposes for which it was collected;
- information will be released to law enforcement upon receipt of a valid judicial instruction;
- compliance with regulatory and legislative requirements is met;
- business damage is minimized by preventing or minimizing the impact of security incidents

3.3. Applicable Laws and Regulations

ECO3 will comply with applicable laws and regulations in the countries and regions where it does business.

3.4. Standards

In order to implement this policy ECO3 has adopted a global risk based approach to information security in line with the Plan-Do-Check-Act (PDCA) principle. ECO3will take into account the following standard:

- 1S0/IEC 27001:2013 Information technology - security techniques - information security management systems - requirements;
- 1S0/IEC 27002:2013 Information technology - security techniques - code of practice for information security management;

3.5. Policy Principles

In order to implement our information security objectives as listed in 3.1, ECO3 has adopted information security policy principles listed below that correspond to the 1S0/IEC 27002 clauses.

3.5.1. Security policy

This policy is the ISP policy of ECO3. Where relevant, it is further detailed in global and / or local guidelines and when applicable, process documents.

3.5.2. Organization of Information Security

3.5.2.1 Internal Organization

Within ECO3, the Executive Management Team (EMT), led by the CEO, is upon delegation by the Board of Directors accountable for corporate governance as a whole. The management and control of ISP risks is an integral part of this corporate governance.

The EMT gives overall strategic direction by approving the ISP principles but delegates tactical responsibilities for ISP to the CFO.

The ECO3 Information Security Officer is responsible for the ECO3 Information Security & Privacy Policy of ECO3 and the tactical coordination of Information Security at ECO3.

The Security Officer is responsible for the Information Security Management System (ISMS), which is part of the overall Integrated Management System (IMS).

The implementation of ISP process documents is under the authority of the operational units (Sales & Services Organizations and Global Support Functions).

The ECO3 Information Security Officer has responsibilities for maintaining the policy and providing advice and guidance on its implementation.

Accountable Management may delegate responsibilities for duties and tasks, but cannot transfer their accountability that the required duties and tasks are executed.

To allow for an efficient and coordinated promotion, implementation and integration of this ISP policy, additional roles and responsibilities may be created throughout the organization.

3.5.2.2 Third Party Management

ECO3 uses the services of a third party service provider through a Master Service Agreement.

ECO3 contractors and consultants shall adhere to and be informed about the ISP policy and process documents. Their employment terms and conditions shall include non-disclosure and confidentiality agreements and/or clauses.

3.5.2.3 Asset Management

An information and information system asset inventory shall be established and maintained. For each asset, or group of assets, a classification identification and ownership shall be defined.

Ownership shall be assigned to an individual with sufficient knowledge and authority about the asset and its role in the business processes of ECO3.

3.5.2.4 Human Resource Security

Specific measurements and guidelines shall be implemented to ensure ISP during the three phases of employment:

- at hiring;
- during employment;
- at termination or change of role and responsibilities.

3.5.2.4.1 At Hiring

Employees shall be informed, upon hiring or change of position within ECO3, about their ISP role and responsibilities in their new function. Possible disciplinary action in case of non-compliance with the ISP policy of ECO3, shall be communicated. Their employment terms and conditions shall include non-disclosure and confidentiality agreements and/or clauses.

3.5.2.4.2 During Employment

Employees of ECO3 shall be made aware of their roles and responsibilities with respect to ISP. Adequate training and instructions shall be provided.

Initiatives shall be taken to ensure the establishment and maintenance of ISP awareness throughout ECO3.

3.5.2.4.3 At termination or change of role

When an employee takes up another position within ECO3 or leaves ECO3, they shall be informed about their ISP role and responsibilities in their new function and the necessary actions shall be taken to ensure the continued protection of sensitive information.

Special attention is needed in order to remove or modify:

- logical access rights;
- physical access rights;
- roles and responsibilities of the function.

When leaving ECO3 or when changing positions, assets owned and provisioned by ECO3, shall be returned.

3.5.2.5 Physical and environmental security

Physical access to the sites and offices of ECO3 and the assets kept in those offices shall be restricted to authorized people only.

Information and information systems shall be protected against unavailability, loss or damage, e.g. through:

- prevention, detection or protection mechanism in case of:
  - fire,
  - theft or loss,
  - water damage;
- an adequate alternative power supply or other measures to prevent disruption.

3.5.2.6 Communications and Operations Management

To ensure the correct and secure operation of information systems, process documents shall be established. No

evidence is required for aspects which are reasonably expected to be known by employees through their logical or repeated use or deduction.

Special attention shall be given to document processes and/or procedures in the area of:

- day-to-day operational service;
- protection against viruses and malicious code;
- roll-out of new software or updates on customer's infrastructure;
- management of logs and audit trails.

Where possible, segregation of duties shall be established.

3.5.2.7 Access Control

To protect against loss, unauthorized change or misuse of information, access to information and information systems shall be restricted using an identification, authentication and authorization mechanism. Full lifecycle ("joiners, movers, leavers") of identities and their authorization shall be maintained.

Access rights to information and information systems shall be assigned on need-to-know or a need-to-do basis. Unique individual usernames shall be allocated in order to allow for non-repudiation of information handling. Where possible, logging and tracking mechanisms shall be used.

Access to both internal and external networked services shall be controlled and strong authentication shall be used to control access by remote users. Connection to ECO3 internal network via public network or dial-in shall be protected appropriately.

3.5.2.8 Information Systems Acquisition, Development and Naintenance

Within ECO3 three kinds of information systems can be distinguished:

- internal IT systems: those used to ensure smooth operations of the different business and supporting processes within ECO3;
- internal Operational Technology (OT) systems: hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events
- customer products and services: those information systems which are designed and built for the support of the business.

All will adhere to sound ISP principles.

3.5.2.8.1 Internal Systems

Information security requirements shall be documented in the specifications of new, or to be modified, information systems and applications. These requirements shall be in line with the private and confidential nature of the processed or stored information and in line with the principles dictated by this document and by regulatory requirements. Special attention shall be given to e.g.:

- access control (authentication and authorization);
- availability of the application and the information;
- logging and auditing capabilities;

Similar considerations shall be made when evaluating a third party's information system and/or application. Any test data shall be made anonymous where reasonably possible.

The principles of access control shall be applied both in the development and test environment.

3.5.2.8.2 Operational Technology Systems

In order to ensure continued operation of processing facilities, ISP measurements or controls shall be included in these systems as of the requirements and design phase. Following ISP controls shall be considered:

- means to protect the confidentiality, integrity and availability of data in transit;
- access control (authentication and authorization), including 3rd party access;
- logging and auditing capabilities.

3.5.2.8.3 Customer Products and Services

In order to deliver secure products and services to our customers, ISP measurements or controls shall be included in these products and services as of requirements and design phase. Following ISP controls shall be considered/

- means to protect the confidentiality, integrity and availability of data in transit;
- strong access control (authentication and authorization) to customer data;
- protected audit and logging for the creation, consultation, modification and deletion of customer data.

3.5.2.9 ISP Incident Management

ISP is established through the safeguarding of the confidentiality, integrity and availability of information and information systems. Any breach of one of these elements can be a threat to ECO3, to the customer or to the customer's customer and is seen as an ISP incident. An incident management system shall ensure the efficient and effective identification, communication, follow- up and resolving of incidents as well as the decrease or avoidance of (similar) incidents. Where possible logging and tracking mechanisms shall be activated.

ECO3 employees shall be informed about the nature of ISP incidents and the procedures to report them. They shall report ISP incidents and known or suspected weaknesses as soon as possible.

3.5.2.10 Business Continuity Management

Disruption of the core activities, caused by major incidents or disasters, can have a significant economic or reputational impact on ECO3. Special attention shall be given to business continuity threats during risk assessments for internal applications as well as customer products and services.

3.5.2.11 Compliance

Legal and contractual obligations shall be respected during the development of the ISP policies and process documents.

To ensure compliance with ECO3's ISP policy, regular verifications and audits are required. Systems and processes shall be analyzed to ensure they meet the expected ISP levels.

4. Policy Review

This policy is reviewed at least every three years or sooner, whenever internal or external changes require an adaptation of this policy.