Eurotransplant Information Security Policy

Document:	ET Information security policy
Version:	1.1
Author:	M. van Hennik
Updated on:	

EUROTRANSPLANT

Change history

Date	Author	Version	Change
01-02-13	M. van Hennik	0.1	New
12-03-13	M. van Hennik	0.2	Changed structure and introduction
20-03-13	M. van Hennik	0.3	Changes following task force meeting on 19 March
03-04-13	M. van Hennik	1.0	Sent to MT for approval
30-5-13	M.van Hennik	FINAL	After comments of Frau Arndt
04-08-14	M. van Hennik	1.1	Revision after evaluation by the working group 8-7-14

Approved versions

Date	Approved by	Version	Signature
17-4-2013	MT	1.0	

Table of Contents

0 Structure of this document

This document contains the information security policy of Eurotransplant. In the appendix a list of underlying documents is added with more detailed policies and procedures regarding information security measurements within the organisation.

To understand the terminology used, the main terms used in this document are briefly explained in section 1. Section 2 is the introduction, setting out the importance, objective and scope of the information security for Eurotransplant. An overview of principles and general basic principles used by ETI for information security is given in section 3. This section describes information security as a quality aspect that plays a role in all processes and applications of ETI.

Section 4 explains how the legislation that relates to the use of data is applied at ETI. The next section, section 5, discusses the way in which statutory regulations and agreements must be observed.

Section 6 provides an overview of the various categories of operating assets distinguished by ETI. Based on these four categories, section 7 presents a number of policy principles, which are refined versions of the general basic principles given in section 3, and which may serve as a reference for the practical implementation of the ISP (Information Security Policy) and the formulation of the measures to be taken in the organisation.

Section 8 describes the PDCA-cycle of the ET information security policy.

1 Terms and definitions

The following definitions apply to this document:

Affiliated third parties: persons who have access (or have an external network connection) to the systems of ETI through information technology

Operating asset: long-lived asset which is used in normal business operations, subdivided into three major categories: property, plant, and equipment (or: fixed assets); natural resources; and intangible assets.

Control measure: a method to control risks, including policies, procedures, guidelines, methods or organisational structures of an administrative, technical, organisational or legal nature

Visitors: persons who visit one of the members of staff of ETI

External members of staff: any person who is not employed by ETI but provides services for ETI on a regular basis (cleaners, consultants, ICT staff, agency workers, etc.)

ISP: Information Security Policy

Internal members of staff: all persons in the temporary or permanent employment of ETI

ISMS: Information Security Management System: that part of a management system which, based on assessment of operating risks, serves to establish, implement, execute, check, assess, maintain and improve information security

ISO-27001: international standard for information technology - security technologies - management systems for information technology

NEN-7510: Dutch standard for medical information - information security in the healthcare sector

PDCA cycle: Plan-Do-Check-Act. The cycle that formulates, executes and evaluates policies and measures, and on the basis of which new basic principles and measures are formulated.

QMS: Quality Management System. This is the system used for the control and evaluation of the quality aspect in the processes of ETI. The ISMS forms part of this.

Risk analysis: an analysis that serves to understand the nature of the risk and to establish the risk level

Risk assessment: the entire process of risk identification, risk analysis and risk evaluation

Software: a set of programs, procedures, algorithms and the documentation in connection with the functioning of a data processing system

2 Introduction

2.1 Information security

The objective of information security is to take and maintain the confidentiality, integrity and availability of information to such levels that any disruptions or problems can be controlled.

Information is an operating asset which, just like other important operating assets, is of value to the organisation and which must be suitably protected at all times. This is particularly important in the ever tighter interconnection of information with automation in society. Due to this increasing interconnection, information is exposed to a rising number and wider range of threats and weaknesses. In addition, the human factor is and remains a weak link in data security. ETI acknowledges that members of staff in general unconsciously pose the biggest risk in terms of information security.

Information can present itself in many different ways. The information may be printed off or written down on paper, stored electronically, sent by mail or electronic media, shown on film or exchanged verbally. Information should always be protected in a suitable manner, taking the form or sharing or storage method into account.

Disruptions to the provision of information and the resulting losses can be prevented or limited by using a suitable set of control measures, including policies, working methods, procedures, organisational structures and software and device functions. Selecting measures to protect information means you have to assess the risks, costs and practical possibilities. These factors change, constantly. The assessment will therefore have to be made over and over again. Information security has an operating process: the ISMS.

2.2 Scope, organisation and ultimate responsibility

The information security policy at ETI relates to participants in the ETI processes, i.e. all internal and external staff, affiliated third parties and visitors, as well as all organisational units and process owners.
The information security policy emphasises all the information systems that fall under ETI's responsibility. This relates to both information generated and managed by the organisation itself and to the process information ETI obtains and manages through third parties.

In terms of continuity and physical security, the policy takes into account a process that goes on 24/7.

Information security is not the same as protection of automation: at ETI, the focus of information security lies on increasing risk awareness in terms of information security of the internal member of staff at ETI.

In order to be able to maintain the ISP to a maximum extent, it is important to clarify the tasks, responsibilities and powers with regard to information security. With a view to the potential impact of disruptions to the continuity of business processes, ultimate responsibility for the policy regarding security and internal monitoring of the information provision lies with the management board of Eurotransplant.

2.3 Objective

The objective regarding information security at Eurotransplant reads:
"to offer a framework of policy principles regarding the exclusivity, integrity and availability of the information provision, in the course of which a balanced (effective and efficient) system of interconnecting measures is developed in order to execute the provision of information in all processes without deviations and to protect it against internal and external threats."

All managers and process owners are responsible for compliance with the policy principle set out in this document when structuring the organisation, processes, working methods and the information systems used in the process thereof.

2.4 Implementation of the policy

The principles mentioned in the information security policy are effectuated in the processes of the organisation. Every process implements principles that are applicable in a manner that fits the specific process.

Adaptations or improvements to the implementation of the principles is responsibility of the process owner.

As part of every project the effectuation of information security principles is taken into account.

The iSec program coordinates the practical implementation of information security projects.

3 General principles and premises

3.1 General policy principles

- At ETI, information security is embedded in all processes and business functions and integrated in the Planning & Control cycle of the organisation. The PDCA cycle is used for the management of an Information Security Management System (ISMS) and to undertake specific actions and projects to improve information security at ETI.
- The ISMS of ETI is based on the standards applied in the ISO-27001 standard.
- Risk management forms part of the ISMS.
- Information security is a quality aspect of the processes, secured in the ISMS. As such the person responsible for the process is responsible for information security.
- ETI uses confidential information (legal term: special personal data). This requires members of staff of ETI to treat information in a specific manner. The security must comply with the applicable legislation, particularly with the Dutch Personal Data Protection Act .
- Information is available only to persons who need it in the course of their position.
- Valuation of information: everyone knows the value of information used in its processes and acts accordingly. How information is treated is determined by its use during the process
- Officers are trained in how to treat information within the process they participate in when performing their duties.
- The systems of ETI comply with the security policy and security standards of the organisation.
- The rules and agreements regarding information security that apply to members of staff of ETI also apply to the affiliated third parties with whom a Shared Services agreement has been taken out.
- ETI owns all the information and software produced under its responsibility.
- ET safeguards that data is used strictly according to instructions of ETI and ETI asks for proof of appropriate information security measures at / by the third party. Affiliated third parties who use the ETI information systems are responsible for the integrity of the information they make available to Eurotransplant.
- During projects, such as infrastructural changes or the acquisition of new systems or changes to a process, information security is taken into account from the start. It forms part of a set of requirements to start a project.

4 Statutory regulations

4.1 Applicable legislation

The legal basis of information security is derived from both relevant national legislation and the legislation of the Member States affiliated to Eurotransplant. In procedures and manuals, Eurotransplant has laid down how members of staff should apply these rules in practice.

Eurotransplant complies with the prevailing organ transplant legislation of the affiliated countries for national donors and recipients in each of those countries.

Eurotransplant processes the personal details obtained within the framework of the aforementioned process in a manner that complies with the Dutch Personal Data Protection Act and the applicable national legislation.

Below follows an overview of the most relevant general legislation in the Netherlands:

4.1.1 Personal Data Protection Act (Wbp)

The Personal Data Protection Act applies to the processing of personal details, automated or otherwise. An important aspect is the purpose limitation and safeguarding of the rights of the parties involved in the processing of confidential medical details. Eurotransplant has implemented the statutory requirements (correctness and accuracy of details and suitable technical and organisational measures against loss and unlawful processing) through its information security policy.

4.1.2 Medical Treatment Contracts Act (WGBO)

The Medical Treatment Contracts Act provides for the use of personal details in the healthcare sector. The Medical Treatment Contracts Act lays down the rights and obligations of both the healthcare providers and the patients. Among other things, this act stipulates that within the framework of treatment, medical details of patients can be exchanged with other healthcare providers who are directly involved in that treatment.

4.1.3 Computer Crime Act

Among other things, the Computer Crime Act focuses on the penalisation of and the fight against crimes committed by means of computer technology and crimes in which (computer) systems are the target. Applying a sufficient security level is made obligatory under this act.
Compliance with this information security policy and implementation of the basic measures at ET should lead to a level of protection that can be regarded as sufficient within the framework of this act.

4.1.4 Copyright Act (Aw)

The legal protection of the copyright of original works, including software, is provided for by the Copyright Act. ETI does not distribute original works without first obtaining consent from the copyright owner. ETI combats the use of software without having the correct licence.

5 Policy with regard to compliance

5.1 Responsibility

Compliance comprises general monitoring of daily practice from the process of quality assurance. Process owners and department managers are responsible for the correct implementation of the business processes assigned to them, and the corresponding provision of information for the correct functioning thereof, and as such also for information security. This means they bear primary responsibility for selecting, implementing and enforcing information security measures and for training and raising awareness among their members of staff.

5.2 Reporting and evaluation

The implementation of information security is evaluated on an annual basis. This is done during the spring, in the form of the Management Board Quality Assessment, of which information security forms a part. The input for the evaluation of the implementation of, and compliance with, the ISP ensues from internal audits and the security incidents reports. The aforementioned PDCA cycle forms part of the ISMS. This system forms part of the Quality Management System of ETI and is embedded in the P&C cycle.

5.3 Information security incidents

ETI ensures that information security events and weaknesses relating to its information systems are reported in such a way that prompt corrective measures can be taken.

- Every information security incident is reported, documented, dealt with and is provided with feedback in accordance with the Incident Management Procedure.
- Reporting back on occurred incidents to the organisation helps to raise security awareness among the members of staff
- The incident management system forms part of the PDCA cycle of the ISMS.

5.4 Non-compliance

Measures may be taken by or on behalf of Eurotransplant in the event of violation of the information security policy and/or the underlying legal provisions.
Within the framework of the collective agreement and statutory provisions, sanctions may be imposed on members of staff who fail to comply with the rules ensuing from the information security policy and/or the underlying legal provisions.
Access to the premises or other operating assets may be denied to external members of staff and visitors who fail to comply with the rules ensuing from the information security policy.

6 Classification and overview of operating assets

Eurotransplant distinguishes different main groups within information security, namely:

1. Technical Infrastructure, including the components:
   - Hardware (servers etc.)
   - Software (such as operating systems, tools, source code)
   - Front-end (workstations, laptops, etc.)
   - Network

2. Physical rooms, subdivided into 4 security zones:
   - Zone 1: open point of contact. A reception desk that is accessible to all during office hours. Reception is manned by a receptionist.
   - Zone 2: authorised personnel or visitors are granted access to the stairs and lift via reception or (not applicable to vistors) by means of key card-secured doors. This refers to all members of staff of all organisations on the premises.
   - Zone 3: ETI's offices. These areas can be accessed by ETI members of staff via zone 2 and visitors (if accompanied by ETI personnel).
   - Zone 4: rooms that accommodate computers and network equipment. Access to these rooms is limited to members of staff from the department responsible for maintenance and management of the equipment.

     Other areas that partially fall under the responsibility of ETI are areas outside the physical offices where people log onto ETI's network, the paper archive and the disaster recovery location.

3. Information with regard to the various business areas, as described in the business function model.

4. Personnel; internal and external members of staff

7 Operating asset management

7.1 Policy with regard to technical infrastructure

7.1.1 IT facilities

- ETI safeguards the correct and safe operation of IT facilities.
- ETI uses common equipment, which:
  - Is used in accordance with the method prescribed by the supplier and in accordance with the conditions;
  - Is supported by the supplier (service agreement);
  - Is replaceable in the short term.
- ETI keeps an updated overview of all the operating assets that are in use.
- ETI holds a legal, valid and authentic licence for all operating assets (equipment, software) that are used for the business processes.
- ETI does not use any equipment or software whose technical lifespan has expired.
- Systems for the support of the primary process are specific to the extent that ETI maintains the required knowledge and expertise at high levels by itself.
- Systems that serve to support the supporting processes are purchased as complete solutions.
- Purchased applications are used in accordance with the functionality offered and are not adjusted specifically for ETI (although they are structured for ETI).

7.1.2 Access security of technical infrastructure

- ETI prevents unauthorised access by users, and damage or theft of information and IT facilities, network services, operating systems and application systems.
- ETI has taken technical measures to safeguard information security when using portable computers and facilities for teleworking.

7.1.3 Information systems

- ETI ensures that security forms an integral part of information systems.
- ETI maintains the security of software exchanged within the organisation and with third parties.
- ETI ensures that the system files are protected.

7.2 Policy with regard to physical security

- ETI prevents unauthorised physical access, damage or disruptions to the premises and the information of the organisation.
- ETI has taken technical measures that even in case mobile operating assets are lost or stolen, information security is safeguarded.
- ETI has taken measures to prevent business activities from being interrupted.
- Rooms that accommodate equipment (computers, communication, power supply, etc.) can be accessed only by members of staff who are required to do so by virtue of their job.

7.3 Policy with regard to information

7.3.1 Process management

- ETI protects information in networks and the supporting infrastructure.
- ETI has taken measures to prevent the unauthorised disclosure, modification, removal or destruction of business assets and prevents business activities from being interrupted.

- ETI offers a suitable level of information security for the agreement regarding third-party service provision.
- ETI safeguardes continuity of the integrity and availability of information. In the event of unforeseen disruptions, the length of the interruption of integrity and availability of the information is kept as brief as possible.
- ETI reduces the risk of a system breakdown to a minimum. A proper planning and preparation of system changes provides sufficient capacity and availability of the resources required to provide the necessary system performances.
- ETI maintains a 'Business Continuity Plan' with a view to business continuity in the event of an emergency.
- ETI ensures that the Business Continuity Plan is regularly tested and maintained so as to ensure it remains up-to-date and effective.

7.3.2 Access security of information

- ETI controls the access to information, with the objective of realising access by authorised users and preventing unauthorised access to information systems.
- Faulty or redundant data carriers are completely wiped before being disposed of.
- Information is available only to persons who need it in the course of their position.
- A policy is in place for the external use of data carriers.
- ETI protects the information it is entrusted with against unauthorised use.
- ETI members of staff are facilitated to work in a safe environment when working out of the office.

7.3.3 Information systems

- ETI maintains the security of information exchanged within the organisation and with third parties.
- ETI protects the confidentiality, authenticity and integrity of information by means of cryptographic resources.
- ETI takes appropriate measures to safeguard that information which has been collected for different purposes may be processed separately.
- ETI reduces risks by internally publishing technical weak spots.
- Data is entered as closely to the (responsible) source as possible.
- ETI provides journaling mechanisms for every (relevant) transaction in the information systems.
- When outsourcing or purchasing services, the data is the property of ETI. Upon termination of an outsourcing contract, all data at a supplier is transferred to ETI in a practical form and destroyed at the supplier in question.
- The results of developments on the instruction of or by members of staff of ETI are the legal property of ETI.

7.3.4 The archive

- Retention periods: ETI applies at least the statutory retention periods for archiving documents (physically or electronically).
- For archiving purposes, dossiers can be converted from paper to electronic form. Exceptions are made for documents that:
  - Represent a (very) high value in terms of the legal onus of proof;
  - Are of special historic value.
- Documents whose contents are included in an automated system are not archived separately if the required retention period is guaranteed by the system in question.
- ETI provides for appropriate procedures and agreements for access to external (physical) archives. These procedures and agreements offer proper protection for the dossiers in those archives.

7.4 Policy with regard to personnel

- Prior to hiring staff: ETI makes sure internal and external members of staff understand their responsibilities and that they are suitable for the roles for which they are being considered, and as such reduce the risk of theft, fraud or the misuse of operating assets.
- All internal and external members of staff sign a confidentiality statement.
- When hired: ETI ensures that all internal and external members of staff are aware of threats and dangers regarding information security, of their responsibilities and liability, and that they are equipped to support the security policy of the organisation in their daily jobs, and to reduce the risk of human error.
- Upon termination of or changes to the employment contract: ETI safeguards that access to the information systems of ETI is blocked when internal and external members of staff leave the company.

8 PDCA cycle

The Information Security Management system is embedded in the PDCA-cycle of the quality management system of ET.

- Information security incidents are reported in the general incident management system
- Information security aspects are audited as part of the internal audit system
- Implementations to increase information security levels and improve the information security policy are evaluated in the annual management review.

Risk analysis is performed periodically in order to adequately monitor the risks and intended preventive measurements with regard to information security.

The iSec program evaluates the scheduled activities of the program at least once a year.

9 Appendix 1

9.1 List of underlying documents regarding information security

- Quality management review
- iSec program
- Annual plans of all departments
- ET Data Policy
- Policy statement Eurotransplant Computer System (in ET manual)
- ET Privacy regulation
- Eurocenter emergency and security regulations
- Continuity procedures Infrastructure
- Continuity procedures Allocation
- ICT System Development: Standards and Guidelines
- Service Level Agreements
- Hiring and outsourcing contracts

- Procedures and regulations for regarding access to the office environment:
    - Procedure provision and management computers and communication devices
    - Regulation camera surveillance
    - Key card regulation
    - Code of conduct use of internet and e-mail
    - Visitors procedure
    - Confidentiality agreement staff
    - Confidentiality agreement third parties