# INFORMATION SECURITY POLICY EUROTRANSPLANT

By Pim Lagrand
Version 1.0

Date of creation: June 14, 2021
Last modified on 17 juni 2021

© Eurotransplant International Foundation. All rights reserved.

## Change history

| Date | Author | Version | Change |
|---|---|---|---|
| 14-06-2021 | Pim Lagrand | 0.1 Concept | New |
| 15-06-2021 | Jorine Petitjean | 0.2 Concept | Review |
| 15-06-2021 | Rene Bouter | 0.3 Concept | Review |
| 17-06-2021 | Serge Vogelaar | 1.0 Final | Official approval |

**© Eurotransplant International Foundation. Alle rechten voorbehouden.**

This document is made available subject to the condition that the recipient will neither use nor disclose the contents except as agreed in writing with the copyright owner. Copyright is vested in Eurotransplant International Foundation, Leiden

# Table of contents

# 1 Preface

Eurotransplant has considered information security as an important issue for years. There must be certainty that information security risks must be acceptable to stakeholders and that measures must be made operational in such a way, that they are not at the expense of the effectiveness, flexibility, and efficiency of the service.

## 2 Responsibilities, objectives, and target audience

In view of the possible impact of malfunctions on the operation and continuity of Eurotransplant and its customers, the final responsibility for information security policy (hereafter: IS-policy) is held by the managing board of Eurotransplant.

The objective of the IS-policy by applying a risk management process is:

> 'Offering a framework of information security principles regarding the confidentiality, integrity, and availability[1] of information provision, with a balanced (efficient and effective) system of coherent developed measures, to protect information against internal and external threats'.

All involved employees must ensure compliance with the principles of the IS-policy when planning the implementation, procedures, methods, and the corresponding information systems that are used. Failure to comply with this policy could have serious consequences for Eurotransplant' s services to its customers and may result in disciplinary action.

[1] Confidentiality: protect sensitive information against unauthorized access
Integrity: ensure that information is correct and complete
Availability: ensure that information is available at the right times

# 3 Scope

This policy applies to all information that is created, received, sent or stored as part of Eurotransplant' s services to its customers and the corresponding contractual obligations. All employees of Eurotransplant must comply with this policy and its application in practice. Deviations must be reported to continuously improve the information security management system. In addition, the policy also applies to contractors who support Eurotransplant in providing services to its customers.

An integral part of this policy is the "Eurotransplant Code of Conduct", to which all employees, contractors and trainees must adhere.

Information security measures based on logical principles are preferred because they are cost-effective and sustainable. These principles are:

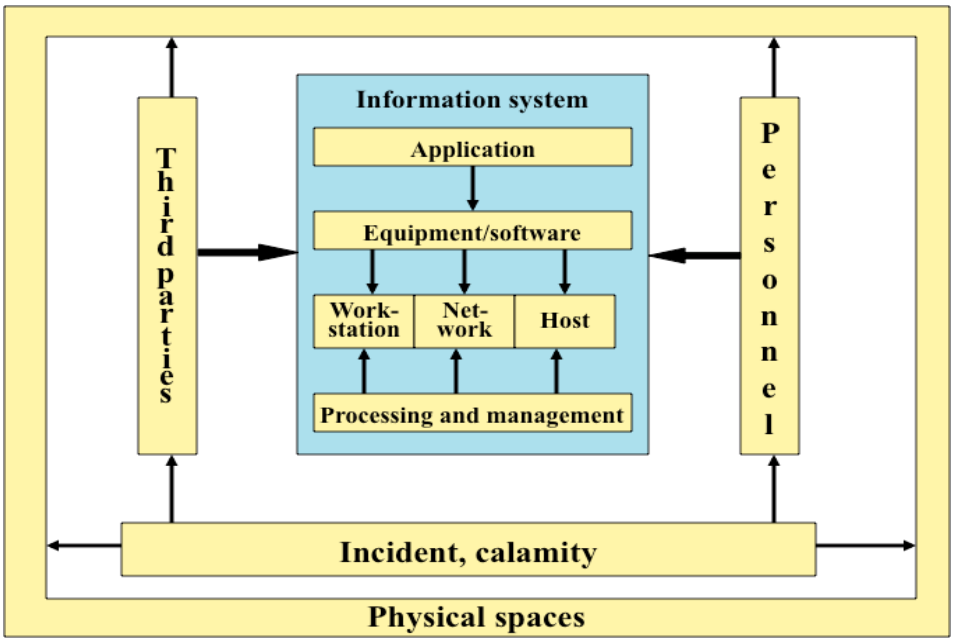
1. Data minimization.
2. Separate sensitive data from other data.
3. Do not move data around needlessly.

All employees are expected to put these principles into practice.

## 3.1 Ownership and scope of the policy

Eurotransplant is responsible for providing its service with adequate security options so that its customers can comply with their applicable information security standards and other laws and regulations. The hosting and management of the software also complies with these requirements. However, this does not release customers from the ultimate responsibility for securing their information.

For each information system, including the corresponding data, a single owner must be appointed. This ownership entails the final responsibility for the system concerned, including determining the risks to be identified with the system, classifying the system and the corresponding data, and developing (or commissioning the development of) adequate means of security and internal control measures. Besides their use, this also involves correct deployment of infrastructural components (workstations, servers, and the internal and external network), accurate processing, adequate management, effective functioning of staff, making agreements with third parties, and providing physical security and facilities to prevent incidents and calamities or to deal with them. All the above-mentioned aspects of infrastructure and management of customers that are not under control by Eurotransplant are included in the figure below.




The term ‘ultimate responsibility' is used because several aspects of the information system are outsourced to other parties, such as Eurotransplant. This does not mean that a maximum level of security is pursued, but an optimal level, so that Eurotransplant can offer services to het customers at an acceptable cost.

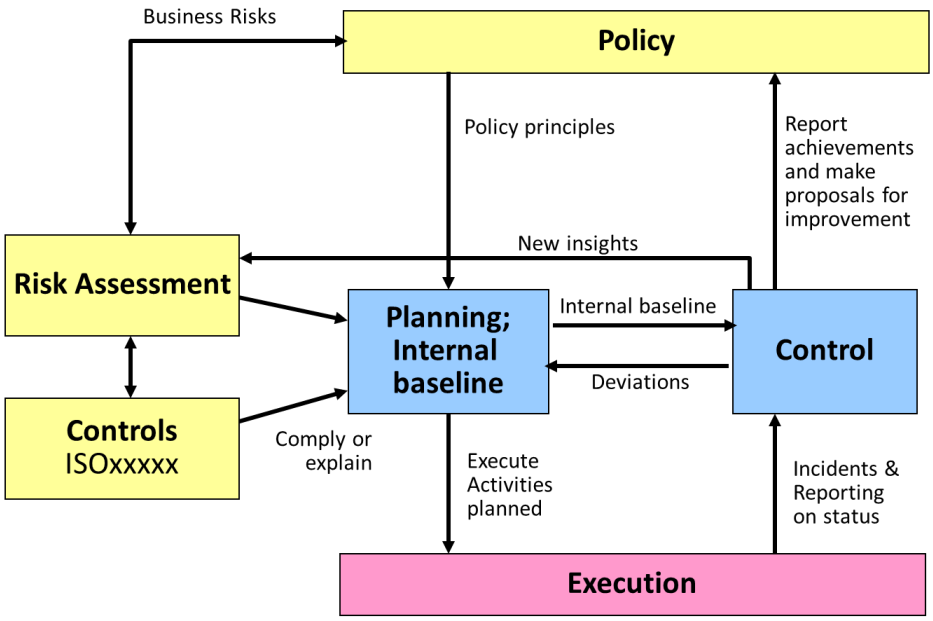
## 3.2 Application of this policy

Based on this policy, risk assessments are conducted, and a set of control measures is defined as a baseline security level, which is the minimum for customer service. In consultation, a higher level of security can be agreed upon with a customer.

## 3.3 Monitoring the operation and compliance with the policy

In the management review, the operation and compliance with the policy are evaluated internally and adjusted if necessary.

An internal audit is conducted annually and reported to management. A component of this internal audit is the re-assessment of risks and an impact analysis of new laws and regulations. The report includes a plan with proposals for improvement. The managing board evaluates the report, approves, or rejects proposals and allocates funding for the realization of the proposals. This process is shown schematically below.




In addition, an annual external audit is performed by an independent third party who is authorized and qualified. The audit report is available for existing and potential customers.

# 4 Policy Framework

In these policy principles, the managing board of Eurotransplant has elaborated how it wants to give shape to information security in a way that is suitable for Eurotransplant.

With the following stated policy principles, Eurotransplant expects to manage its information security risks while at the same time maintaining its flexibility and efficiency in the performance of its activities.

The policy principles bridge the information security risks and the security objectives and measures of the baseline security level of Eurotransplant.

Moreover, the policy principles provide the framework for the managing board for setting information security objectives, which are appropriate for Eurotransplant.

The policy principles apply to those data operations for which Eurotransplant is legally and / or contractually responsible.

In the further implementation of this policy, the following principles should be applied:

1. Information security is an important business risk for Eurotransplant. The management board therefore determines the policy, assesses the risks, approves the control measures, ensures that the resources needed for the information security management system are available and has internal and external assessments carried out at planned intervals to ensure that the information security management system continues to work adequately and is improved where necessary.
2. Regarding information security, Eurotransplant conforms with prevailing legislation and the contractual obligations with customers and business partners.
3. Eurotransplant continuously endeavors to improve the services to its customers.
4. The security objectives and measures of the NEN-ISO/IEC 27001 standard and the privacy guidelines of the Dutch Data Protection Authority, to the extent they contribute to the information security of Eurotransplant and are enforceable, form the basis for the measures to be taken. This is mainly a cost benefit consideration.
5. Eurotransplant regards cybercrime as an undesirable social problem and sees it as its duty to take appropriate measures to minimize damage caused by criminal activities.
6. For Eurotransplant, trust is an important asset, and it applies the principle of reciprocity to employees, customers, suppliers, and other stakeholders. Eurotransplant assumes that they comply with agreements regarding the confidentiality, integrity, and availability of information.
7. The HRM policy is also aimed at improving the confidentiality, integrity, and availability of information among employees. This is discussed during a periodic evaluation.
8. The physical security of the buildings and the spaces therein guarantees the confidentiality, integrity and availability of data and data processing including the supporting assets.
9. The development or purchase, installation and maintenance of information and communication systems, as well as the integration of new technologies, must be carried out with additional measures, if necessary, in such a way that this does not compromise information security.
10. Assignments to third parties involves measures to prevent any breach of confidentiality, integrity, and availability of information.
11. When processing and using data, measures are taken to safeguard the privacy of customers, employees, and other stakeholders.
12. Logical access control ensures that unauthorized persons or processes do not gain access to the information systems, databases, and software of Eurotransplant.
13. External data provision is done on a 'need to know' basis. Internally, this is not always convenient, because knowledge sharing is essential for a cost-effective service to customers.
14. Eurotransplant and its employees take measures to prevent confidential data from getting into the hands of third parties.
15. Input from customers that contains confidential data is securely archived or destroyed shortly after processing.
16. Data transfer is covered with security measures to prevent a breach of the confidentiality and integrity of that data.

17. Authorized employees must also have secure remote access to the relevant operational environments. No confidential data is stored outside of the operational environment, but exceptions are possible under certain conditions.
18. Operational environments are separated from other environments; within these operational environments, specific access rights may be granted, and access can be monitored.
19. The management and storage of data in operational environments are such, that no data can be lost, unless there is a force majeure.
20. Job segregation has been made between the respective organizations for development, administration, and use. Moreover, segregation of duties is applied wherever possible and desirable.
21. A process is in place to deal adequately with incidents and to learn lessons from them.
22. Contingency plans and arrangements are in place to ensure the continuity of information provision.
23. In case of outsourcing data processing, the managing board may decide to temporarily deviate from these principles and accept the risks involved.
24. In case of conflicts, the mission of Eurotransplant prevails over the requirements set by information security and privacy.
25. Information security is an integral part of the design, development, and management of software, even if it is developed by third parties. Security by design and privacy by design and default are the main engineering principles here.
26. Eurotransplant and its employees realize the sensitivity of the personal data that they process and guarantee the protection, rectification, and transparency of this data always, in order to protect the privacy of the data subject.