1 Background

The management of Human Heroes recognizes that the increasing use of data communication options via the internet, the complexity of and interwovenness between automated systems, the massiveness of daily communication, the size of the files as well as the increasing professionalization of computer crime lead to a great dependence and vulnerability of the automated information provision within the organization. The risks associated with this are very significant and can pose a threat to the confidentiality, integrity and continuity of the automated information provision and thus indirectly to the image and therefore the continuity of Human Heroes.

2 Final responsibility

Regarding the possible impact of disruptions on the continuity of Human Heroes, final responsibility for the security and internal control policy of the automated information provision lies with the management of Human Heroes.

3 Objective and target group

This by-law is part of the overall security policy of Human Heroes. The objective of the by-law on the confidentiality, integrity and continuity of the automated information provision of Human Heroes is: "Providing a framework of policy principles relating to the exclusivity, integrity and availability of the automated information provision, in which a balanced (effective and efficient) system of interrelated measures is developed, in order to protect the automated provision of information against internal and external threats."

The supervisor must ensure that the policy principles formulated in this by-law are met at the institution.

4 Involved organizations

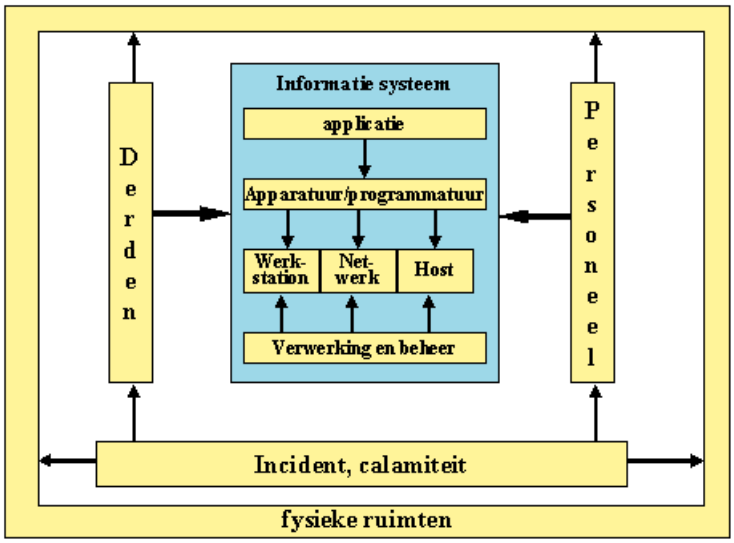
- Security organization.
- The user organization is and remains, as the holder, ultimately responsible for the used automated information systems
- The system development organization is responsible for realizing the desired functional specifications during system development processes.
- The processing organization is the holder of the agreed technical infrastructure, including the infrastructural security means.

5 Information security design

For each automated information system, including the associated data, one holder must be explicitly appointed. The holdership implies the final responsibility for the system in question, including the determination of risks to be identified by the system, the classification of the system and the associated data, and the development of adequate security resources and internal control measures.

In addition to the application, this also involves the correct use of the infrastructural components (workstations, servers and LAN / WAN), the correct processing, the adequate management, the proper functioning of each employee, making agreements with third parties, physical security and facilities for prevent or deal with incidents and calamities.

In the figure below all mentioned sub-areas of an information system are included.



Areas of attention security

A final responsibility is mentioned because a number of aspects of the information system are outsourced to other holders. This can relate to aspects during the development of the system, as well as during the management, use and / or certain sub-components of the total system.

The measures to be taken, as well as the prioritization thereof, must be determined on the basis of a periodically draft risk analysis by the business unit, in which: the threats against reliable and continuity-oriented, automated information provision and the related risks are recognized and a balanced system of interrelated measures is being developed to reduce the risks at acceptable costs. Therefore, a maximum level of security is not sought, but an optimal level.

6 Policy principles

- The physical and logistical security of the computer systems of Human Heroes is such that the confidentiality, integrity and availability of the data and data processing are guaranteed.
- Purchasing, installation and maintenance of these data-processing systems, as well as the integration of new technologies, must not compromise the level of safety of the total information provision.
- The employee policy is partly aimed at contributing to the confidentiality, integrity and continuity of the information provision.
- Assignments to third parties for the performance of work are surrounded by measures in such a way that no breach of the confidentiality, integrity and continuity of the information provision can occur.
- Development and maintenance of information systems take place within the frameworks and rules of the established ICT architecture according to a standard methodology, whereby the documentation is established according to a fixed system.
- Strict divisions between the test / development environment and the production environment have been made with the automated information provision.
- Separate segregations have been made between the system development, management and user organization.
- When processing and using data, measures are taken to ensure the privacy of customers.
- Logical access security ensures that unauthorized persons or processes do not have access to the automated systems, data files and software of Human Heroes.
- Data provision internally and externally takes place on the basis of 'need to know'. Every employee takes measures to prevent information from falling into the hands of people who do not strictly need this information. Access to information systems is also adequately secured according to this principle. An exception is made for the ICT administrator role in order to achieve better service to the users.
- Data transport is protected by security measures such that no breach can be made of the confidentiality and integrity of the data and the provision of information as a whole.
- End-user computing is surrounded by such measures, that the confidentiality and integrity of the delivered information.
- In order to prevent computer virus infections, only authorized versions of (legal) software are used.
- The management and storage of data is such that no information can be lost.
- There is a process to deal with incidents adequately and to draw lessons learned here.
- There are contingency plans and provisions to ensure the continuity of operations and the provision of information and to prevent reputation damage.