Information Security Policy

Introduction

Baggerbedrijf de Boer is a medium-sized dredging company, located in Sliedrecht. The activities consist of dredging and carrying out measurements and other hydraulic engineering work in the broadest sense of the word. This work is carried out worldwide.
Baggerbedrijf de Boer strives to provide a high-quality service and to take all measures necessary to ensure the safety of its own employees and of third parties and to prevent (im)material damage. Part of this is to bring information security to such a high level that all data management risks are calculated and the organization regularly evaluates and, if necessary, adjusts the information security policy.
Baggerbedrijf de Boer has been considering information security as an important issue for many years, in which it must be ensured that risks must be acceptable to the customer and that measures must be made effective and without compromising the effectiveness, flexibility and efficiency of the service.

Responsibility, objective and target group

In view of the possible impact of disruptions on the business operations and continuity of Baggerbedrijf de Boer and its customers, the final responsibility for the information security policy rests with the management of Baggerbedrijf de Boer.
The Policy information security (hereinafter referred to as policy IS) aims to control the risks regarding the availability, integrity and confidentiality [1] of the information provision within Baggerbedrijf de Boer and we define as follows:
“A framework of policy starting points on the confidentiality, integrity and availability of information provision, within which a balanced (effective and efficient) system of interrelated measures is developed, in order to protect the provision of information from internal and external threats”.
All parties concerned must ensure that the policy principles set out in this document are met in the organisation, procedures, working methods and the information systems used.

Scope

This policy applies to all information created, received, transmitted or stored in the services of Baggerbedrijf de Boer to customers and the related contractual obligations and supporting processes. The policy and its elaboration apply to all employees of Baggerbedrijf de Boer. Deviations from this must be reported, so that the management system is continuously improved. In addition, the policy also applies to contractors, who support Baggerbedrijf de Boer in its services to customers.
An inseparable part of this policy is the **"Code of Ethics",** which all employees, contractors and trainees must also adhere to. As much as possible, security measures are sought based on logical principles, because they are cost-effective and sustainable. These principles are:

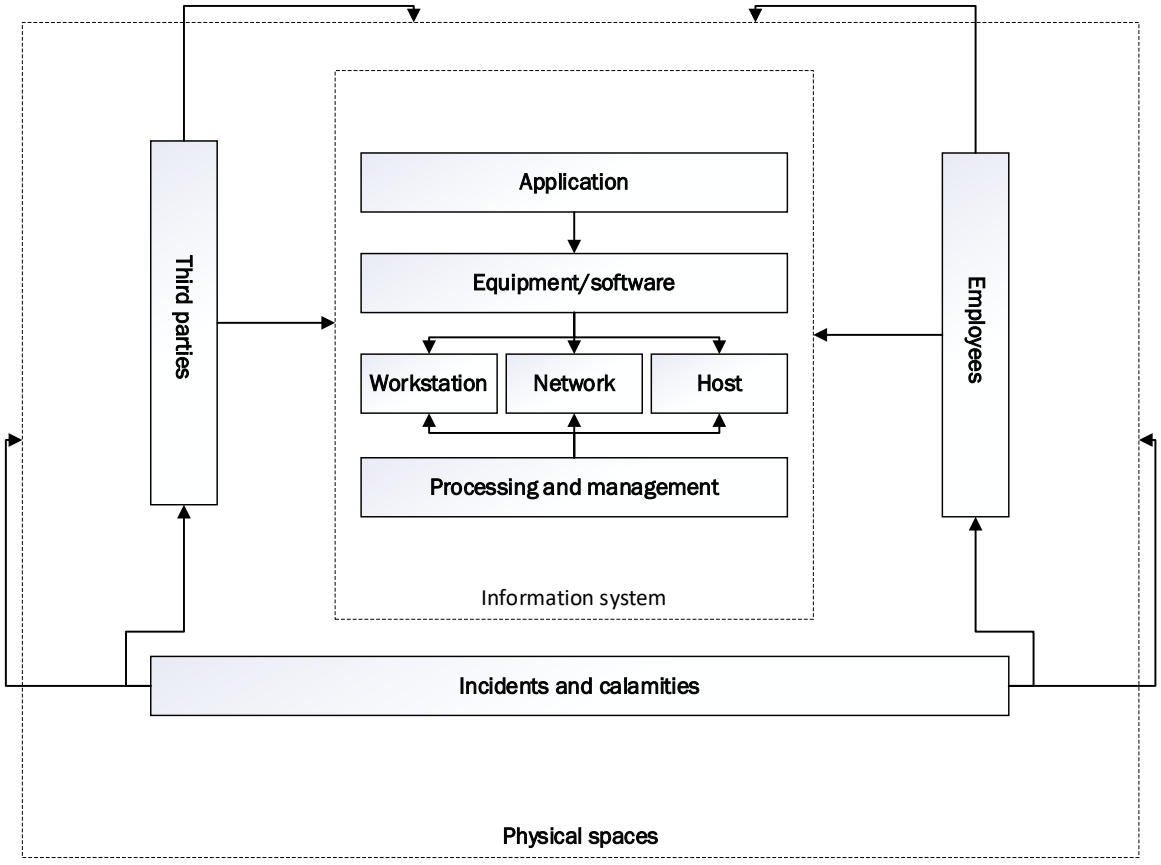
1. You don't have to protect confidential information that you don't have.
2. Do not drag with confidential data.
3. Separation of data.

All employees are expected to put these principles into practice.

[1] Availability: Ensure that information is at the right times present is.
Integrity: ensure that information is correct and complete.
Confidentiality: protect sensitive information from unauthorized knowledge.

Holdership and scope of the policy

Baggerbedrijf de Boer is therefore responsible for making its service available with sufficient security options, so that its customers can comply with the IB standards and other laws and regulations applicable to it. The hosting and management of the software also meets these requirements. However, this does not relieve the customer of the ultimate responsibility for the security of its information provision.
Each information system, including the associated data, must be explicitly named as one holder. The holding implies the ultimate responsibility for the system in question, including determining the risks to be recognised by the system, classifying the system and the associated data and developing adequate security tools and internal control measures. In addition to the application, this also concerns the correct use of the infrastructural components (workstations, servers and the internal and external network), the correct processing, the adequate management, the proper functioning of the personnel, making agreements with third parties, physical security and facilities to prevent or deal with incidents and calamities. The figure below shows all the areas mentioned in an information system.



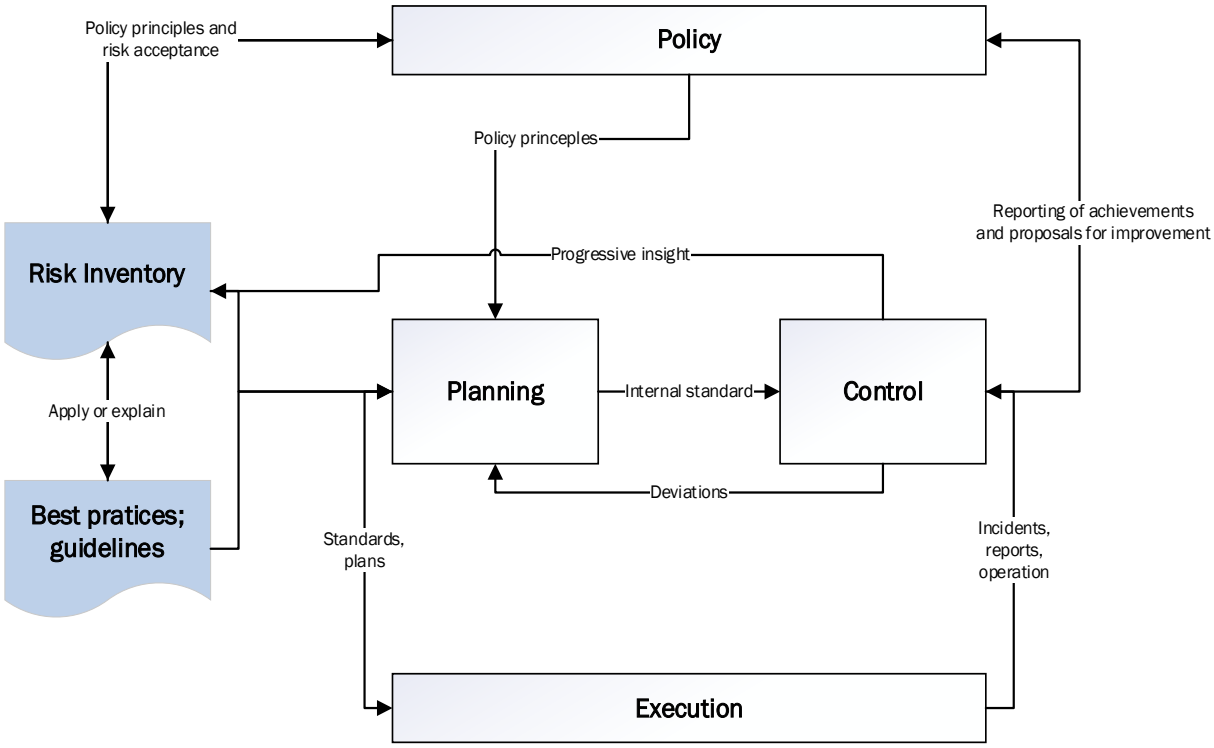
There is talk of ultimate responsibility because a number of aspects of the information system are outsourced to other holders such as Baggerbedrijf de Boer. This does not aim at a maximum level of security, but an optimal level, so that Baggerbedrijf de Boer can offer its services at an acceptable cost.

Elaboration of this policy

Based on this policy, risk analyses are carried out and a set of measures is defined as an internal standard, which counts as a minimum level of security for the provision of services to customers. In consultation, a higher level can be agreed with a customer.

Policy monitoring and compliance

The management assessment shall evaluate the operation and compliance with the policy internally and, if necessary, adapt it.
An internal audit is carried out annually. Part of this internal audit is the reassessment of risks and an assessment of new contracts and laws and regulations. Part of this report is also a plan with improvement proposals. The management assesses the report, approves proposals or does not approve them and allocates a budget for the realization of the proposals. This is shown schematically below.



In addition, an annual external audit is carried out on the functioning of the IB management system by an independent third party, who is competent and competent for this purpose. The reporting of this is available to (potential) customers.

Policy starting points

With the following qualitative policy starting points , Baggerbedrijf de Boer expects to manage its information security risks while maintaining its flexibility and efficiency in carrying out its work.
The policy starting points are the bridge between the information security risks and the management objectives and measures from the Internal Standard of Baggerbedrijf de Boer.
The policy starting points also provide the framework for the management , in which it wants information security objectives to be and shaped, which are appropriate for Baggerbedrijf de Boer.
These policy starting points apply to those data operations, for which Baggerbedrijf de Boer is legally and/or contractually responsible.

The following principles apply in the further implementation of this policy:

1. Information security is an important business risk for Baggerbedrijf de Boer. The Management Board therefore adopts the policy, assesses the risks, determines the measures, makes sufficient resources available and periodically has the functioning of the policy and compliance with these measures assessed internally and externally to ensure that the IB management system continues to operate adequately and, where necessary, improves.
2. Baggerbedrijf de Boer complies with the relevant legislation and contractual agreements with customers and business partners with regard to information security.
3. Baggerbedrijf de Boer strives to continuously improve its services to customers.
4. The management objectives and management measures of the NEN-ISO/IEC 27001 standard and the privacy guidelines of the Dutch Data Protection Authority (AP) form the starting point for the measures to be defined, insofar as they contribute to the information security of Baggerbedrijf de Boer and are enforceable. This is mainly a business economic consideration.
5. Baggerbedrijf de Boer considers computer crime to be an undesirable social problem and sees it only as its task to take appropriate measures to limit damage caused by criminal activities as much as possible.
6. Trust is a great asset for Baggerbedrijf de Boer and it applies the reciprocity principle to employees, customers, suppliers and other stakeholders. Baggerbedrijf de Boer assumes that they are fulfilling agreements with.b.t. availability, integrity and confidentiality of the provision of information.
7. The HRM policy is partly aimed at improving the availability, integrity and confidentiality of the provision of information to employees. This will be discussed during an annual evaluation.
8. The physical and logistical security of the buildings and the spaces therein are such that the availability, integrity and confidentiality of the data and data processing including the assets are guaranteed.
9. Development or purchase, installation and maintenance of information and communication systems, as well as the integration of new technologies, should be carried out, where necessary, by additional measures, without prejudice to information security.
10. Assignments to third parties for the performance of work are surrounded by measures in such a way that there can be no breach of the availability, integrity and confidentiality of the information provision.
11. When processing and using data, measures are taken to ensure the privacy of customers, employees and other data subjects.
12. Access security ensures that unauthorized persons or processes do not have access to the information systems, data files and software of Baggerbedrijf de Boer.
13. External data is provided on the basis of 'need to know'. Internally, this is not always desirable because knowledge sharing is essential for a cost-effective service to customers.
14. Baggerbedrijf de Boer and its employees take measures to prevent confidential information from ending up in the hands of third parties.
15. Input from customers that contains confidential data is archived or destroyed at short notice after processing.
16. Data transport is designed to cover security measures in such a way that no breach of the confidentiality and integrity of this data can be committed.
17. Authorized employees must also have remote secure access to the production environments relevant to their production. No confidential data is stored outside the production environment. Under conditions this can be deviated from.
18. Production environments are separate from other environments and can be granted specific access rights and access monitoring is possible.
19. The management and storage of data in production environments are such that no information can be lost unless there is force majeure.
20. Functional separations have been made between the development, management and user organization. Furthermore, function separation is applied where possible and desirable.

21. There is a process to deal with incidents adequately and to draw lessons learned from them.
22. There are emergency plans and facilities to ensure the availability of the information provision.
23. In the event of outsourcing of data processing, the Management Board may decide to temporarily deviate from these policy starting points and to temporarily accept the risks thereof.
24. In the event of conflicts, Baggerbedrijf de Boer's mission prevails over the requirements set by IB and or privacy.
25. Information security is 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 starting points.
26. Baggerbedrijf de Boer and its employees realize the privacy sensitivity of the (special) personal data that they process and guarantee at all times the blocking, correctability and transparency of this data in order to protect the privacy of the data subjects.

Statement of Applicability (SoA)

The organization wants to meet the requirements of the ISO 27001 standard. This manual contains the documents “QHSE-03.01.0004 Relationship Table ISO 27001” and “QHSE-03.01.0040 Statement of Applicability ISO 27001 and Annex A” with version date 01-01-2025 which describes how the requirements of the standard are integrated into the management system. This creates a single integrated management system for the entire organisation for quality and information.
Measuring the results of information security processes is expressed in several documents. The criteria for risk acceptance or their mitigations are set out in document QHSE.03.06.8020 FMEA Information Security. This also describes the method of risk analysis and stakeholder analysis.

Sliedrecht, 1 January 2025

Drs. C.J. van de Graaf
Director

Ir. H.C. van de Graaf
Director