Information and Security Management Policy

This document sets out the information security policy for Onnec Group. All managers must read the policy and make their staff aware of how it affects them and the duty of care it imposes upon every employee.

Information is vital to Onnec Group and our customer's businesses; the policy describes Onnec Group's commitment to the protection of all information. Adherence to this policy is not optional and every endeavour must be made on behalf of the company to ensure that information is protected.

- The Directors and Managers responsible for Onnec Group's service delivery recognise the need to protect the company's information assets and those of its customers, to which it has access. They are fully committed to the adoption, implementation, maintenance, and continuous improvement of standards of the organisations Information Security Management System (ISMS).
- The organisation shall as necessarily provide appropriate security education, training, and awareness of information security management, to ensure compliance with the requirements of the ISO/IEC 27001 standard.
- The organisation shall endeavour to ensure compliance with legislative, regulatory, and contractual requirements always.
- Business continuity will be a priority of Onnec Group and appropriate planning will be in place to deliver business continuity.
- Known information security violations will be reported and documented in accordance with the requirements of the ISO/IEC 27001 standard.
- Employees within Onnec Group have major influence upon information security both within Onnec Group and within customer organisations and shall act in accordance with the organisations policies & procedures as well as applicable law, British and International Standards.
- The scope and depth of this information security policy will be reviewed annually by the quality team, unless there is a notable change in the company's business, which would cause an earlier review to be appropriate.
- Certification to ISO/IEC 27001 shall be maintained and implemented in the true spirit of the standard.
- The company will strive for continual improvement of its services in line with customer requirements, British and International standards, and legislation.

Our key security objectives are as follows:

- Confidentiality: Protect sensitive information from unauthorised access or disclosure. This includes safeguarding personal data, trade secrets, and proprietary information.
- Integrity: Ensure the accuracy and reliability of data. Prevent unauthorised modification, deletion, or corruption of information.
- Availability: Ensure that critical systems and data are accessible when needed. Minimise downtime due to security incidents or technical failures.
- Authentication and Authorisation: Implement strong authentication mechanisms to verify user identities. Control access rights based on roles and responsibilities.
- Risk Management: Identify and assess risks related to information security. Develop risk treatment plans to mitigate or accept these risks.
- Incident Response: Establish procedures to manage security incidents promptly. Detect, respond to, and recover from breaches or vulnerabilities.
- Compliance: Adhere to legal, regulatory, and contractual requirements related to information security.

Our framework for Setting Security Objectives is as follows:

- Context Analysis: Understand our organisation's context, including its business goals, stakeholders, and risk appetite. Consider legal, industry, and organisational requirements.
- Risk Assessment: Identify and assess risks to information assets. Evaluate the impact and likelihood of threats. Prioritise risks based on their significance.
- Risk Treatment Plan: Develop a plan to address identified risks. Define security controls, policies, and procedures to mitigate risks effectively.
- Performance Metrics: Set measurable objectives for each security goal. For example, reduce the number of security incidents by 20% within the next year.
- Continuous Improvement: Regularly review and update security objectives. Monitor progress, analyse performance metrics, and adapt as needed.

The policy is applicable to all information held within Onnec Group. Much of this information is held on computer systems and networks operated by or on behalf of Onnec Group. All such systems are covered by this policy. Its purpose is to support the welfare of the Company, its staff and, where applicable, its customers and suppliers by protecting the confidentiality, integrity and availability of information held.
The Board of Onnec Group fully endorses the policy and is committed to supporting its implementation throughout.

For and on behalf of
Onnec Group

Philippe Huinck
CEO

13th November 2024