Information Security Policy Summary

1. Introduction

1.1. This document summarizes the **Information Security Policy,** which outlines the fundamentals for Intellicene's Information Security Management System (ISMS).

1.2. The company's management has established and approved the policy, expressing its commitment to protect the business and personal information of the company, its employees, and its customers.

2. Background

2.1. Ensuring ongoing and reliable operations by Intellicene (hereafter, *the company*) is affected by and dependent on the levels of confidentiality, integrity, availability, and resilience of the information assets under the company's responsibility.

2.2. The information, the systems used to manage it, and its technological infrastructure are essential company assets that must be protected like other valuable resources.

2.3. Compromising that information would cause damages that may have operational, technological, and financial impacts on the company, along with damage to its image and reputation and its employees' privacy.

2.4. The company's infosecurity policy assumes dynamic security risks and is tailored to its operational and organizational requirements. Its guidelines form the basis for working procedures in the various infosecurity areas.

2.5. The company's infosecurity policy is derived from the international ISO 27001: 2013 Information Security Management Standard.

3. Managerial Commitment to Infosecurity

3.1. Intellicene's management (hereafter, *the management*) considers data protection a top priority.

3.2. The management undertakes to lead all implementation and education activities required to realize appropriate data protection as required by the law, regulations, and the ISO 27001 certification.

3.3. The management will allocate the resources required to protect the company's information assets and meet the Information Security Management System (ISMS) required by ISO 27001.

3.4. Employees must be aware of infosecurity risks and take all necessary steps to prevent a data breach or other security incidents; they must also report any such incident to the company's infosecurity officers.

4. Company Information Security Objectives

4.1. Ensuring the confidentiality of sensitive information of Intellicene customers and employees stored in IT systems and facilities.

4.2. Securing the availability of information and IT systems to ensure operational and business continuity and continued customer service.

4.3. Securing the integrity of information throughout the work processes within Intellicene. Ensuring reliable and accurate results are provided in all activities and processes, emphasizing core processes related to Intellicene business activities and customers.

4.4. Securing the business information relevant to Intellicene products, operations, and services.

4.5. Securing Intellicene employees' personal data and maintaining their confidentiality.

4.6. Meeting mandatory information security regulations and guidelines and customers/stakeholders' requirements.

4.7. Raising the awareness of information security among managers and employees.

4.8. Enhancing the resilience and recovery of Intellicene information systems and networks regarding compromise of confidentiality, reliability, and availability resulting from malicious action(s) by external or internal threats.

5. Risk Assessment

The infosecurity policy principles will rely on a risk management system to identify, control, minimize, or prevent the security risks that are liable to affect the information and information systems.

6. Responsibilities

The following individual employees and company units are responsible for implementing this security policy:

6.1. An infosecurity steering committee is in charge of setting company infosecurity goals and policies and ensuring implementation and proper management of the information security management system.

6.2. Chief Information Security Officer (CISO) is responsible for the ongoing management of infosecurity in the company.

6.3. Company managers and employees are personally responsible for maintaining information security and confidentiality.

7. Activity Areas and Infosecurity Rules

To meet the management's infosecurity responsibility and commitment, the following rules have been outlined for each of the following activity areas:

7.1. **Logical security** is the main protective layer closest to the information stored in IT systems. CISO will determine the level of logical security required for the various components of these systems. An access authorization and control policy will be applied in keeping with 'employees' roles and on a need-to-know basis.

7.2. **Physical security** will be implemented to prevent actions that could result in the exposure, theft, modification, or destruction of information in line with the classification level of the information in question.

7.3. **HR infosecurity** principles have been determined to reduce the risks related to employee reliability issues, lack of employee awareness, or deliberate attempts by employees to compromise the company's information and information systems.

7.4. **Secure development** aspects are integrated into IT system development processes.

7.5. **Purchasing and vendors.** Infosecurity aspects of communication and interaction with third parties and contractors are implemented.

7.6. **Backup.** The company has defined processes to ensure the reliability, integrity, and availability of information to ensure that the various types of information in the company have been identified and that the backup requirements for each type of information are defined according to information sensitivity.

7.7. **Access control.** Rules and principles for providing access to information systems and controlling access have been determined.

7.8. **Encryption mechanisms** have been integrated into company systems to protect sensitive information against exposure and modification.

7.9. **Remote access** to the company's network by employees and third parties will be enabled and controlled according to infosecurity guidelines.

7.10. **Mobile devices.** The company's infosecurity principles and guidelines are implemented to secure the use of laptops and other mobile devices.

8. **Executive management considers all company managers, employees, and contractors (full/part-time) fully invested in protecting its information and expects full cooperation in implementing this policy.**

Sincerely,

Alan Stoddard – CEO