Information Security Policy

Itiviti Group AB

Table of Content

Note on Confidentiality

Classified: Public

This document is classified as Public and may be freely shared, both internally and externally.

There may be requests by external entities regarding further details with regards to Itiviti Group's information security program. On such occasion, there may be a need to disclose selected parts of our Information Security Manual, which are classified as Sensitive. Therefore, such disclosure shall only be made after it has been internally approved, and after the recipient has signed a Non-Disclosure Agreement.

Any personal interference with this policy instruction may cause a disciplinary action to be undertaken.

Introduction

Based on the ISO/IEC 27001:2013 information security standard, Itiviti Group ("Itiviti") has produced the following Information Security Policy in order to demonstrate the company's approach and commitment to this matter.

Why Information Security?

Information is a very significant business asset for Itiviti and therefore needs to be protected. Information exists in many different forms. It can be provided verbally, be written on paper, be stored electronically, be on film, or transmitted digitally. Irrespective of the way information may exist, be stored or transmitted, it must be protected in an appropriate manner.

Itiviti requires information security to mitigate security risks to information assets. It is critical to protect the company's proprietary and sensitive information to maintain a competitive advantage in the marketplace, to ensure profitability, and to secure and maintain customer and partner trust and confidence.

Security threats originate at a wide variety of sources, including computer-assisted fraud, industrial espionage, sabotage, vandalism and natural disasters. Computer viruses, unethical hacking and denial of service attacks are examples of threats encountered while operating over the Internet.

These types of threats are becoming increasingly more common, more ambitious and more sophisticated.
Therefore, Itiviti's overall information security objectives are as follows:

- To have well-functioning information procedures within its operations and activities
- To proactively identify and mitigate security risks to the organization's information assets
- To ensure customer trust by providing assurance about the company's products and services

– To ensure the company's long-term growth, competitiveness and survival.

What is Information Security?

According to ISO 27000:2014 detailing the international standard's vocabulary, information security is "[the] preservation of confidentiality, integrity and availability of information", thus outlining three general objectives for protecting information. These objectives are defined below.

Confidentiality

Confidentiality is achieved by ensuring that information is accessible only to those authorized to have access. If an unauthorized person, computer system, process, or other entity gains access to information (either voluntarily or involuntarily), confidentiality is compromised.

Integrity

Integrity is achieved by safeguarding the accuracy and completeness of information and processing methods. Integrity can be compromised through malicious altering (e.g. attackers manipulating details of financial transactions), accidental altering (e.g. transmission errors, a hard disk crash), or programming errors resulting in data inconsistencies.

Availability

Availability is achieved by ensuring that authorized users, systems and processes have access to information and associated assets when required.

Philosophy of Protection

Itiviti's philosophy of protection provides the intent and direction behind the company's protection policies, guidelines and standards, and is comprised of three principles:

1. Security is everyone's responsibility. Maintaining an effective and efficient security posture requires a proactive stance on security issues from everyone. Security is not "somebody else's problem"; Itiviti employees are responsible for adhering to the company's security policies and guidelines, and to take issue with those who are not doing the same.
2. Security permeates the organization. Security is not just focused on physical and technical "border control". Rather, Itiviti seeks to ensure reasonable and appropriate levels of security awareness and protection throughout its organization and infrastructure.
3. Security is a business enabler. A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for the company. Security has a direct impact on Itiviti's viability within the marketplace, and must be treated as a valued commodity.

These principles are mutually supportive; ignoring any one in favor of another may undermine Itiviti's overall security posture.

Success Factors

The following factors are critical to a successful information security program within Itiviti:

- Policies, objectives and initiatives that clearly reflect Itiviti's business objectives and corporate culture
- Highly visible support from Itiviti's board of directors and executive management
- Solid understanding of risk management practices and information security requirements
- Documented guidelines, standards, and procedures providing support to Itiviti employees
- Effective communication of, and guidance on information security to all relevant Itiviti stakeholders
- Information security awareness training available to Itiviti employees and consultants
- Continual review and measurement of the effectiveness and efficiency of security controls and mechanisms
- Annual policy review to reflect changes to business objectives or the risk environment.

Applicability

This policy shall apply to all companies within Itiviti and shall be followed by all employees as well as, when applicable, by partners and suppliers (including consultants). The policy covers all information, handling of information, and all information systems within Itiviti.

Other steering documents related to information security, such as the Data Protection Manual and Information Security Manual, are available on the Itiviti Intranet.

Review and Evaluation

This policy shall be reviewed at least annually and updated in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new laws and regulations, or changes to the organization's infrastructure.

Reviews shall include an assessment of the policy's effectiveness based upon:

- The nature and number and impact of recorded security incidents.
- Cost and impact of controls on business efficiency.
- Effects of changes to technology.

Owner

Chief Financial Officer.