The Helsinki Regional Transport Authority

Information security policy

22 March 2018

Version 1.1

Document management

Document name	HSL_tietoturvapolitiikka_22032018.docx
Version:	1.1
Document owner:	Information Security Manager
Author:	Kim Nordström
Quality assurance/approved by:	Hannu Heikkinen
Approval procedure:	The document does not have a formal signature section. It is subject to approval in accordance with HSL’s applicable approval procedure. Information about the most recently approved version is available from the document owner.
Availability of the applicable version:	The most recent applicable version is available from the document owner.
Validity of the document	The document is valid after it has been approved. The document is evaluated, maintained and approved annually.
Distribution:	Public
Document model prepared by:	Arto Viljanen CISM, CISA, CRISC
Document model owned by:	HSL
Keywords:	Information security, management system, information security policy

Document change history

Version	Change date	Maintained by	Change	Approval
0.1	17 January 2017	Arto Viljanen CISA, CISM, CRISC, Visma Consulting Oy	First working version/draft of the information security policy	
0.9	20 January 2017	Arto Viljanen CISA, CISM, CRISC, Visma Consulting Oy	Commented and maintained version of the information security policy	
1.0	25 January 2017	Hannu Heikkinen	Version markings	HSL Management Group
1.1	22 March 2018	Kim Nordström	Updated according to the annual schedule	

HSL’s information security policy

HSL’s information security policy defines the key information security principles and requirements with regard to the business.

Information security at HSL means ensuring the confidentiality, integrity and availability (usability) of data (ISO/IEC 27002). Good information security represents high-quality operations and is an important part of risk management. Maintaining a standard of information security that is appropriate, balanced and adequate in terms of HSL’s business enables the continuous use of modern and efficient business processes and methods.

The administrative and technical measures required for information security and other necessary procedures are implemented using solutions that are justified and proportional to the threats and risks facing HSL’s operations.

In terms of HSL’s information security, the key targets for protection are people, premises, devices, telecommunications, information systems, services, and data and data materials in all formats throughout their life cycles.

Alongside this document, the framework for HSL’s information security work is set by Finnish law, HSL’s strategies, regulations and internal instructions, the ISO/IEC 27001 & 27002 standards, and good practices in the sector.

HSL’s information security organization ensures the confidentiality, integrity and availability of data with the help of the information security management system (ISMS; ISO/IEC 27001). The information security management system defines and documents HSL’s information security organization, leadership and management practices, detailed information security duties and responsibilities for every member of the information security organization, and policies and principles for each area of information security. Information security work is led by the information security manager. At HSL, this duty is discharged by Kim Nordström.

HSL’s information security risks are evaluated regularly and specifically in conjunction with new systems and major changes.

Information security obligations apply to the personnel of HSL’s partners in the same way as to HSL’s own personnel. Every member of HSL’s personnel, HSL’s partners’ personnel and parties otherwise operating on HSL’s behalf are provided with regular information security training or instructions as is necessary with regard to handling their work duties. The information security manager is responsible for arranging training.

HSL’s information security is audited as part of normal auditing procedures. The information security manager regularly reports to HSL’s senior management on the state of information security.

Every member of HSL’s personnel and of HSL’s partners’ personnel is obliged to report any information security deficiencies, threats or procedural faults that they detect to their line manager or HSL’s information security manager.

Information security matters are communicated on HSL’s intranet, Rinkeli, as required. The information security manager is responsible for communications.

Helsinki XX Month 2018

Suvi Rihtniemi Hannu Heikkinen

Executive Director Director of Department, Technology Solutions