

Supplier company

Distribution address

Postal code and CITY

Country

Processor/Official

DATA SECURITY MANAGEMENT

Common guidelines:

Appendix

The City of Helsinki's data security instructions for the supplier

The City of Helsinki's data must be adequately secured

The Supplier must protect the data related to the City of Helsinki against abuse, distortion, unauthorised use as well as to ensure the availability of the data when they are needed. The data must be secured in the provision of services as well as technical information and communication systems. The Supplier shall comply with the provisions on good data processing practice and data protection as required by the current legislation in regard to personal data and other data processing. The Supplier shall also provide its personnel and service providers with instructions on these matters.

This document provides general data security guidelines that can be supplemented by an agreement-specific description of the exact data security arrangements. These instructions apply to the Supplier regarding the processing of the City of Helsinki's data. The data security arrangements for technical information and communication systems are described as part of the system description.

The Supplier shall require its subcontractors who are involved in the processing of the City of Helsinki's data to meet the same data security requirements as the City of Helsinki requires of the Supplier.

Description of the Supplier's data security management

The Supplier can demonstrate its administrative data security by using a data security management system which is in accordance with a quality system. In data security management, the following requirements apply to the Supplier.

General principles of the Supplier's data security

The Supplier must be able to present the general principles of data security that have been approved by its management, which have been provided to the Supplier's personnel and subcontractors. These principles can be in the form of a document called Data Security Policy, Data Security Guidelines or Data Security Principles.

Systematic data security management

The duty responsibilities related to securing data and technical information and communication systems have been defined. These can be described in the quality system or in the form of a manual on operations.

DATA SECURITY MANAGEMENT

The Supplier's service providers

The Supplier's data security management comprises its own subcontractors, whose work the Supplier is responsible for in the same way as for its own work. This can be demonstrated with agreements and in the general principles of data security.

Inspection right

The City of Helsinki has the right to inspect the Supplier's data security management regarding the processing of the City's data. The Supplier is responsible for ensuring that such inspection can be extended to the subcontractors used by the Supplier. The inspection of the data security management also covers the activities related to data processing as well as the inspection of the technical information and communication systems.

Personnel involved in successful data security management

The Supplier's human resources management procedures contribute to data security management. The Supplier must be able to demonstrate how its human resources management is organised. This can be demonstrated with a manual on human resources management or work instructions.

Personnel's data security expertise

The Supplier must provide the personnel involved in the processing of the City of Helsinki's data with adequate training that takes data security expertise into consideration. This applies to those personnel who have access to the information and communication systems that provide service to the City of Helsinki or to the facilities where service is provided to Helsinki. The Supplier must be able to demonstrate that the personnel have adequate training to process the City of Helsinki's data. The personnel's competence can be demonstrated with task-specific certificates of professional competence, lists of participants in training sessions or course material used in the Supplier's training programmes.

Ensuring the reliability of the personnel and confidentiality obligation

The Supplier must be able to inform the City of Helsinki of the persons who have access to the City's data.

The Supplier must have a defined procedure to be used for ensuring the reliability of persons processing the City of Helsinki's data or who have access to the facilities where service is provided to Helsinki. The procedure may involve being subject to a security clearance procedure.

The Supplier must inform the personnel that the confidentiality obligation remains in force by law even after the end of employment.

Former employees of the City of Helsinki's service production

The Supplier must immediately terminate the user rights to the City of Helsinki's data of all persons who are no longer working for the Supplier or in services related to the City. The Supplier must ensure that these persons return all such work equipment that contain the City of Helsinki's data.

If an employee of the Supplier had been granted user rights or access rights to other systems or facilities of the City of Helsinki, the Supplier must immediately report that the employee no longer works in the City of Helsinki's service production and that the employee's user rights have been terminated.

DATA SECURITY MANAGEMENT

Confidentiality management, secrecy

The Supplier may only process the City of Helsinki's data for the purpose agreed with the City. The City of Helsinki's data may not be processed, stored or sent to anyone in any way other than as agreed with the City and when it is necessary for the production of service for the City.

Guidelines on maintaining confidentiality

The Supplier must have written instructions for its personnel and subcontractors on maintaining data confidentiality and secure data processing.

Encryption of recordings and data communications

In the City of Helsinki's services, passwords and the like must always be stored in encrypted form. Passwords, PIN codes, private keys or other similar data must not be stored without encryption.

The City of Helsinki's confidential data must be encrypted when it is stored on portable storage media, such as USB devices or mobile devices. The choice of the encryption method must be justified either by a risk assessment related to the operating environment in question or by the recommendations issued to the public administration. The safe handling of backup copies must also be demonstrable.

The Supplier must always transfer the City of Helsinki's confidential data in the information networks using encryption, such as VPN, HTTPS, SFTP or the like. The City of Helsinki's confidential data must not be transferred in the open information network without encryption. This requirement also applies to system login information. The choice of a technical protection solution must be justified either by a risk assessment related to the operating environment in question or by general recommendations related to the technology used.

Reliable destruction

The Supplier must destroy the City of Helsinki's data reliably after the City has asked for the data to be destroyed when they are no longer needed and the retention period requirements allow it. This requirement also applies to the physical devices that are to be decommissioned and that contain the City of Helsinki's confidential data. Reliable destruction can be demonstrated with work instructions and records of the destruction.

Protection of the working space

The Supplier must arrange the facilities for the processing of the City of Helsinki's data in such a way that they are well protected. The adequacy of the security solutions used in the facilities and IT equipment premises can be justified by comparing the solutions with the VAHTI recommendations for working spaces (2/2013 Information security guidelines for working spaces, <https://www.suomidigi.fi/en/ohjeet-ja-tuki/vahti-instructions>)

The starting point of the processing facilities for confidential data is that the working space has basic-level security. However, the requirements of the advanced-level working space must be taken into account in the working space if the premises are used to process, for example, special categories of personal data, sensitive data, data subject to non-disclosure or other data, the unlawful disclosure or unauthorised use of which may result in damage or even significant damage to the public or private interest. Such data could concern the security arrangements in buildings, establishments, structures

DATA SECURITY MANAGEMENT

or information and communication systems or preparedness for accidents and exceptional conditions. The Supplier must have a risk assessment of the processing facility for confidential data.

It is essential that the working space allows the storage of the City of Helsinki's data only with those authorised to process them and that the destruction or loss of the data is prevented.

User rights are personal

The Supplier must use personal usernames in all the systems that provide service to the City of Helsinki. It is prohibited to use shared and common usernames unless their use can be identified. If the provision of the service requires using shared usernames, the principles of using the usernames must be approved in writing by the City of Helsinki. The principles of using shared usernames must identify which personal username has been used or who has used the shared username. This can be demonstrated with principles of use, work instructions and user records (logs).

Administrators

Administrator credentials may only be used exclusively for maintenance tasks, troubleshooting and at the request of the City of Helsinki. The user may only log in to the system with the administrator credentials in situations where the user must perform maintenance tasks, troubleshooting or when carrying out a commission by the City of Helsinki. The use of the administrator credentials only for maintenance tasks, troubleshooting or commissions by the City of Helsinki can be demonstrated with principles of use, work instructions or user records (logs).

Strong identification

If the identification of the user is based only on knowing the username and password, it is necessary for the passwords to be strong enough (at least 10 characters and at least 15 characters for the administrator).

Secure work in service production

The security of the Supplier's service production can be demonstrated with valid quality certificates and it can be accompanied by a supervisory function that covers the services (data security control centre, cyber security centre).

Protection of terminals

In the case of laptops or similar devices, the City of Helsinki's data must be protected with usernames and encryption. This can be done by encrypting the operating system's own disk.

Software updates

Updates to devices or systems must be installed without undue delay, especially with regard to security updates. If the installation of the updates needs to be delayed, the Supplier must take the necessary alternative measures to reduce the risks. The alternative restriction measures can be justified with the recommendations in the vulnerability updates of the Finnish Transport and Communications Agency's Cybersecurity Centre.

When missing device updates result in a security risk to the City of Helsinki's data or the systems that provide service to Helsinki, this is a security incident to the Supplier. The Supplier is responsible

DATA SECURITY MANAGEMENT

for ensuring that the updates to the devices under the control of the Supplier or its subcontractors have been installed.

Security software

The Supplier must use up-to-date anti-malware software in those environments where suitable protection is available for the City of Helsinki's service. The Supplier must monitor and ensure that the security software works and is up to date.

The Supplier must use and maintain a firewall or similar data protection solution for all such devices that can be connected directly to the public network and that are directly or indirectly related to the processing of the City of Helsinki's data. Such a device can be an expert's laptop which should be protected against both harmful data communications and malware ("viruses").

Securing servers

All default passwords used in the systems that provide service to the City of Helsinki must be changed. No default passwords can be left unchanged. It is also recommended to change the default administrator credentials. In other words, it is advisable to replace the management or administrator credentials with other credentials.

The City of Helsinki reserves the right to carry out a technical vulnerability inspection of the system in a manner agreed with the Supplier.

The City of Helsinki does not accept or approve a system and its delivery if the system contains critical vulnerabilities. Critical vulnerabilities can refer to critical faults listed in the vulnerability updates of the Finnish Transport and Communications Agency's Cybersecurity Centre or critical faults according to the update recommendations for the device or software in question. A critical vulnerability poses a serious risk to the intended use and data, and the Supplier must be able to demonstrate by means of a risk assessment as to why an issue that appears to be critical does not actually pose a risk if it is to remain in the system.

The system description must indicate which devices and software the implementation of the service involves. The descriptions must cover hardware, system software and software versions with such precision that the service can be implemented with the help of the descriptions.

It is recommended to harden the servers by applying the installation instructions commonly used in the sector. Examples of such instructions include NIST, SANS and instructions from device or system manufacturers. The purpose of the hardening instructions is to improve the server's resilience to security attacks or other threats.

When a vulnerability is detected, the Supplier must start remedying the vulnerability without undue delay and inform the City of Helsinki of it.

Logs

The system logs (user records) must cover the needs of the service or data processing provided to the City of Helsinki. There must be instructions for the management of the logs. The logs must always be stored in such a way that they remain reliable. When examining the logs, a copy of them from a trusted storage location must always be used.

DATA SECURITY MANAGEMENT

Typically, it must be possible to use the logs to track changes, additions and deletions to data or system components. In particular, it must be possible to use the logs to view or make data to be protected available, such as personal data which are considered sensitive.

It must be possible to use the logs to monitor system activity. This can be made possible by using an application programming interface (API), through which the logs can be linked to an external monitoring system. At its simplest, it must be possible to browse the logs when the system is active (online).

Incident management

The Supplier must have a well-defined procedure for managing security incidents that affect the City of Helsinki. Incident management can be demonstrated with work instructions and a work-flow system (ticketing system).

The Supplier must report to Helsinki without undue delay all such incidents where:

- The confidentiality, integrity or availability of data related to Helsinki, such as personal data, has been compromised; or
- The security of the services provided to Helsinki has been compromised.

All incidents must be reported to the contact person assigned by the City of Helsinki for cooperation.

Supervision performed by Helsinki

The City of Helsinki reserves the possibility to collect usage data (logs) of the user of the City's information network and information and communication systems to troubleshoot and investigate security incidents and to form a general picture of the situation in the City's information resources management.

Contact information and service monitoring

The contact persons of the service or system, the methods of communication and the methods of monitoring the service must be recorded and shared to all parties. For the sake of communication of security issues, it is important to record the contact information of the security managers or their respective contact persons as well as the procedures related to incident management.