Effective as of: 28 October 2020	Confirmed by: Chief Information Security Officer Riitta Gröhn

A8 ASSET MANAGEMENT

CONTENTS

1 Asset management

‘Assets’ (*suojattava omaisuus*) refers to data and information systems in the possession of or under the responsibility of Aalto University, and to the related processes, systems, hardware, servers, terminals, software and information networks. ‘Assets’ therefore refers not only to assets owned by Aalto University, but those for which Aalto University bears responsibility.

The personal data of employees, for example, is not a possession owned by Aalto University, but Aalto University as the controller has responsibility for protecting the data and thus they are regarded as Aalto University assets.

2 Management of assets

Aalto University’s information systems, as assets, are, by default, specific and itemised in the configuration management database (CMDB). CMDB maintains the information of asset items throughout the asset lifecycle.

Aalto University's Records Management Plan identifies the datasets processed at the university.

3 Parties responsible for assets

Parties responsible are designated as having the responsibility for assets. Head of Service is in charge of assets.

3.1 Responsibilities concerning assets

The owner of an asset to be protected has responsibility for implementation of information security and data protection in accordance with legislation, information security and data protection rules and binding instructions for the lifecycle of the asset, from its introduction until its withdrawal from service. The binding instructions for information security management systems as well as other guidelines and rules provide a more detailed description of the asset owner's responsibilities.

3.2 Delegation of responsibilities

Duties related to responsibilities may be delegated to other persons or outsourced to third-parties providing that the delegate has adequate authorisation and resources. The responsibility itself, however, may not be delegated.

4 The processing and handling of assets

4.1 Obligation to follow regulations

As the owner of information systems and services, Aalto University has, on the basis of its supervision and monitoring rights, the right to issue regulations on the appropriate purposes and use of the IT services intended for work and studying. The obligatory nature of the regulations is, insofar as necessary, incorporated in cooperation agreements with partners and in procurement requirements.

The regulations include the binding instructions given by Aalto University IT Services or by other Aalto University units. Best practices and legislation must also be followed.

The regulations concern:

a) all members of the university community
b) other users of Aalto University information systems
c) Aalto University units
d) the workstations in by the general public at Aalto University
e) all devices connected to the university network

Regulation monitoring

IT Services (the information security group and IT solution owners), asset owners, and (administratively) supervisors hold responsibility for monitoring in their respective areas.

Consequences of actions contravening information security and data protection
Persons are individually responsible for all consequences and damage caused by their actions (see the Policy of sanctions for IT offences at Aalto University).

Agreements will make note as necessary of any cases of persons to whom the normal practices for noncompliance would not apply. Instructions in cases of persons performing non-military service will follow the guidelines for civil servants.

4.2 Acceptable use of assets

4.2.1 Information systems

The university's information systems are intended to be used for studying, teaching, research, artistic creation, and administrative tasks at Aalto University.

Private use is allowed to a reasonable extent and only if it does not:
a) interfere with the other uses of the system;
b) cause needs for changes to the university information systems;
c) contradict with the general binding instructions or those on the use of an individual system or with other information security documentation; or
d) contravene the law or is contrary to best practices.

Examples of permitted private use include private emails and the use of other online services unrelated to work duties.

Other use than that mentioned above requires written authorisation from the IT director. Authorisation requires justifiable grounds.

Note the following in particular.
a) Commercial use for promoting anything other than the university is forbidden, unless specifically authorised.
b) Use for political activity (such as election campaigning) is forbidden, unless as regards university elections, the operations of political student organisations/guilds and trade unions of the staff, and professional interaction with society.
c) Use for proclaiming religious or similar convictions is forbidden.
d) Publishing, forwarding or distributing illegal material or material incompatible with good practice is forbidden.
e) Putting unnecessary strain on the system is forbidden.

f) Access rights may not be used to search for or use information security holes and a user's own login may not be given to another party.
g) Data communications may not be copied or altered.
h) Systems, directories and services may not be breached.
i) Acquisition or attempted acquisition of data from an information system without authorisation is forbidden.
j) Using, saving or distributing information that was received accidentally or was addressed to or rightfully belongs to others is forbidden.
k) Any observed or suspected shortcomings of information security and misuse must be reported to the chief information security officer without delay (information security incidents).
l) Setting up service processes visible beyond the workstation or server requires authorisation from the person in charge of operations.
m) Only university owned or administered devices may connect to a wired university telecommunications network.

4.2.2 Terminal devices

A guide to the approved use of date terminal equipment (DTE) is contained in Aalto University's Terminal device rule. The main principle is that DTEs administered by the university should only be used to process Aalto University information for e.g. performing work duties.

When using a DTE to process Aalto University information, the user is obliged to ensure the information security of the equipment physically (e.g. locking it when leaving unattended; see A11) as well as digitally (e.g. identifying emails that contain malware).

4.2.3 Datasets

Observe the instructions on the processing of datasets. In addition to personal data, users should follow the university's more detailed instructions on the processing of personal data. These are found on aalto.fi.

The Records Management Plan (TOS) also sets data obligations on users. Particular datasets must be sent for archiving in the digital system for managing documents and records, for example. Agreement and contracts, for their part, are usually sent to the Registry.

Separating private from work-related material
The material in the home directory of a student is always interpreted as private. However, staff must keep their private material (such as private emails and files) clearly separate from work-related material.

Persons who have more than one role, e.g. both an Aalto student and an employee, should see primarily to their obligation to follow the regulations concerning them as Aalto University employees (for instance, the obligation of secrecy).

4.2.4 Portable external memory devices

Portable external memory devices are governed by Aalto University's rules for the classification and processing of datasets. Possessors of portable media are responsible for following the rules. Datasets to be protected may only by exception be stored on portable media and then only if encrypted according to the A10 Instructions on obligations.
Should a portable external memory device be missing, report this immediately to the information security team (security@aalto.fi).

When using Aalto University data, you must take into consideration the obligations of secrecy and the prohibition against using the information for private gain. The abovementioned may, depending on the case, be statutory obligations or be based on agreements entered into by Aalto University.

In the case of employees, consideration should be given particularly to the employee's obligation of loyalty, i.e. not to act contrary to the interests of the employer.

4.3 Secrecy

Employees have an obligation of secrecy regarding information that is received at work is it to be kept secret.

Students do not have a general obligation of secrecy. However, a student may have an obligation of secrecy if information that is to be kept secret comes to his/her knowledge through his/her serving in a position of trust. Students may also have a requirement to be bound to secrecy regarding a private project for their studies. Pursuant to legislation on the secrecy of communications, students have an obligation of secrecy concerning messages they inadvertently received that were intended for another person.

As for other parties, Aalto University observes secrecy in the agreements it enters into if necessary, e.g. if the party in question does not for some other reason already have a secrecy obligation.

5 Returning assets

All employees, students and Aalto University external users are expected to return all Aalto University assets in their possession at the end of their assignment, employment or student relationship or agreement. They must return borrowed devices, however, already before leaving according to the rules for borrowing the devices. Unreturned

assets will be handled as an Aalto University information security incident.

The obligations relating to the return of assets is described in more detail in separate guidelines, as needed.

In all cases, however, returning assets refers to at least the following.

- When leaving the organisation, the individual must return any access cards or other devices borrowed.
- Data resources must be returned. Data resources on the individual's personal device must also be returned.
- Individuals must delete their private email and files before their access rights to the information system are revoked.
- Individuals must remove all software that has been provided by the university for home use on the basis of membership in the university community when their right to study or employment relationship ends, unless otherwise stated in the licence agreement of the software.
- As for other licences, they should be removed or returned to Aalto University. The same applies to licensed usernames, which must be deleted from the system. The owner of an asset to be protected has a responsibility to review their licences annually.
- To the extent necessary, work-related messages and files must be transferred by a member of staff to a person agreed upon with the supervisor. For operational continuity, all essential information should be transferred. This applies also to, where applicable, to students who have worked in research groups, for example. In must be ensured that all essential data resources be transferred to Aalto University and deleted from the individual's own device.

The obligation to return is not absolute, but deviations from it are allowed only on justifiable grounds or as permissible according to legislation or the terms of licence.

Deviations from the rules presented above may be possible in the following cases.

- Licences: Individuals must remove all software that has been provided by the university for home use on the basis of membership in the university community when their right to

study or employment relationship ends, *unless otherwise stated in the licence agreement of the software*.
- The obligation of return or removal generally does not apply to course material, such as lecture slides, received by students during their time of studies.

As regards third parties (e.g. representatives of suppliers), they should transfer or destroy the data associated with a user account for the purpose of executing a project in the manner specified in the project contract. Parties to an agreement with Aalto University must inform the relevant persons in charge of operations of the end of the agreement period.

In returning assets, consideration should also be paid to secrecy or other obligations that remain beyond the end of the employment or other relationship (e.g. student relationship) such obligations must be agreed and communicated as necessary (see the A7 Binding instructions).

6 Moving physical data media

Media and devices containing information (e.g. laptop computers, smartphones, servers, USB flash drives and backup media) must be protected against unauthorised access, misuse and data corruption during the time the device is being moved, with consideration given to Aalto University's rules for classifying and processing datasets and as needed to the documentation on information security (e.g. instructions on telecommuting).

Activities involving the use of data media are monitored for e.g. information security as part of the normal operations of the university. Possessors of data media are responsible for following Aalto University's information security and data protection documentation in their use of the media.

7 Destruction of data media and datasets

Media that are no longer needed and/or have reached their expiration data must be destroyed in adherence with the Aalto University's rules for the classification and processing of datasets, taking also into consideration the requirements of the Act on the Openness of Government Activities (621/1999) and the archives act (831/1994). The system owner (owner of an asset to be protected) and the possessor of data media are responsible for following the rules and regulations.

Follow Aalto University's Records Management Plan when destroying a dataset.