Entry into force: 1 October 2020	Confirmed by: Chief Information Security Officer Riitta Gröhn

A9 ACCESS CONTROL

TABLE OF CONTENTS

1 General goals of access control

Access to data and information systems is limited. Data and information systems are also protected by limited access to the physical spaces where data and information are processed.

Only those who have access rights have the right to use the information systems of Aalto University (public services excluded) and, even then, only to the extent that they need to access the data and the systems. Access rights are always connected to a username.

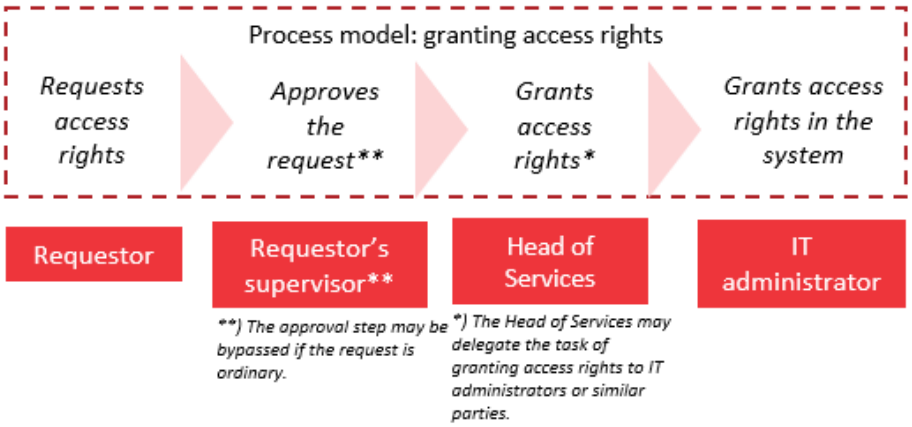
Different kinds of usernames are described in the section ‘Usernames’ below.

Access to spaces where confidential data or devices are kept is also limited. Examples of such spaces include data centres and the rooms where data centre services are maintained. Access to these spaces is only granted to persons whose task or job description makes it necessary. In addition, appropriate physical access control is ensured. Special restrictions apply to some areas. For details, see A11 Physical and environmental security.

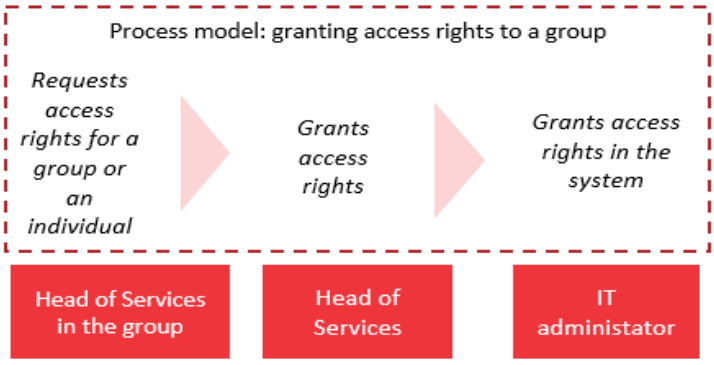
1.1 Authority to grant, edit and revoke access rights

The authority to grant, edit and revoke access rights is vested in designated persons only. Only specifically appointed persons have the right to register users and grant, edit and revoke access rights at Aalto University. The person granting access rights to a resource must be authorised by Head of Services.

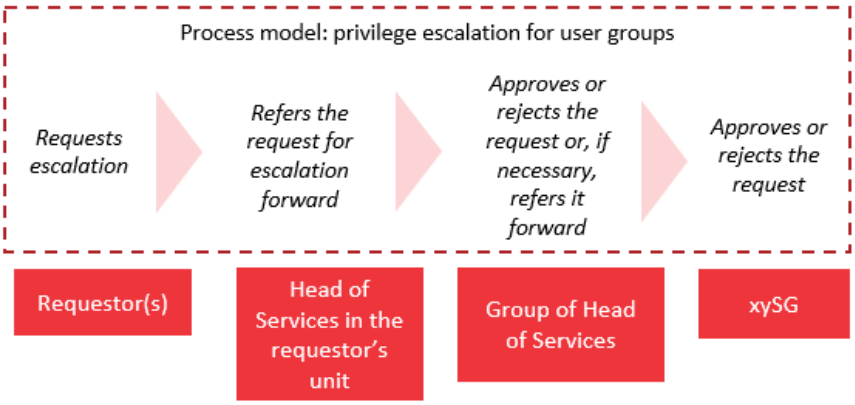
a) The process of granting access rights to a user



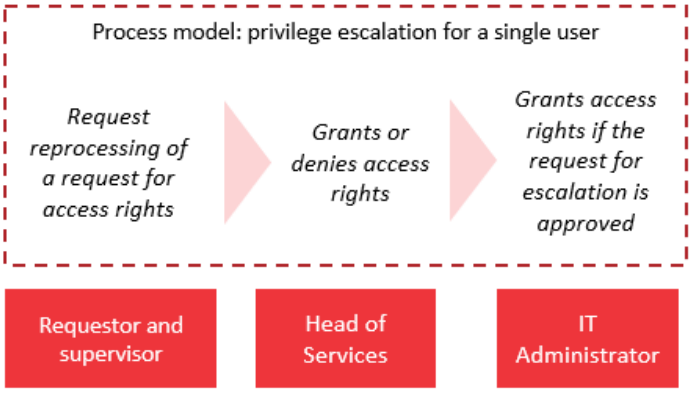
b) The process of granting access rights to a group



c) Privilege escalation process for groups



d) Privilege escalation process for a single user



The process models in sections C and D above describe a situation where the request of a user or a user group for access to data or an information system has been denied. In the escalation process, a Head of Services, then a group of such persons, and (if required) a steering group reprocess the request for access.

The policy of granting of access rights to physical spaces that contain protected property is described in the Instructions on obligations, document A11.

1.2 Revocation and editing of access rights

The revocation of access rights prevents the user from accessing networks, online services and information systems. The editing and revocation of access rights are governed by the principles described in this document in the section 'Revocation and editing of access rights and usernames'.

The editing or revocation of physical access rights prevents access to physical spaces. The revocation process of these access rights is described in the document A11. In principle, changes to logical access rights may necessitate changes to physical access rights.

1.3 Documented and transparent access control process

Access rights to data and information systems are edited and revoked in accordance with a written process.

The access control process is transparent. This means that any decisions on access control may be communicated to the parties necessary. The purpose of transparency is to guarantee uniform decisions on access control.

1.4 Bypassing access control with administration and maintenance applications

Access to all systems, also for maintenance purposes, is usually governed by access control, as this makes it possible to connect a user to their actions. If it is necessary to bypass access control or use applications to do so, such activities must be kept to a minimum.

1.5 Password use

The password management system must require the use of strong passwords. All users must use individual passwords of high enough quality. Read more about the quality criteria in the password guidelines. Passwords may not be reused, and the user must be forced to change their password at certain intervals and whenever necessary. The user must make sure that no other person knows their password. Storing passwords as plain text in systems is prohibited, and passwords may only be sent as encrypted emails.

The user must change the password immediately upon first log-on, unless a technical solution (e.g. password.aalto.fi) has been used to hand over the password to the user, meaning that no one else knows it. In any case, the password must be changed regularly and whenever necessary, for example, if it is suspected to have fallen into some other person’s hands.

1.6 Server certificates

Server certificates are used, renewed and deactivated in accordance with written instructions. A list of existing and deactivated certificates is kept.

1.7 Protection of source code and configurations

Access to program, system and device source codes and configurations must be limited to protect their integrity and

confidentiality. Logs must be kept of all changes to source codes and configurations, and the log chain must be stored in line with the Aalto University Log Management Policy.

1.8 The purpose of access control logging and the protection of logs

Access control must maintain a sign-in log that makes it possible to connect users with their activities. The process of collecting logs is laid down in the Aalto University Log Management Rule.

The main principle is to keep logs that are extensive enough to make it possible to detect security breaches or attempts thereof, and to document such breaches afterwards. The logs must be protected, and editing them afterwards must be prevented. The storage of logs is also governed by the Log Management Rule.

2 Username

2.1 Personal usernames

a) Access rights are personal and tied to unique, individual usernames
Usernames make it possible to connect users with their actions, placing responsibility on the users. In addition, a person's access rights to individual systems can be investigated by looking at their username.
Usernames may be used for private purposes within a reasonable limit, but some restrictions have been placed on this kind of use. The restrictions are described in detail in the Binding instructions, document A8. In principle, browsing the Internet is permitted, for example.

b) Users must be reliably identified
Before an Aalto IT account can be created for a user, they must be reliably identified. An acceptable means of identification it to use an official form of identification or online identification using Aalto University's online service.

c) Usernames and passwords are handed only to users who have verified their identity
Usernames and passwords (whether new, temporary, or replacements for old ones) can only be handed to persons who have verified their identity through strong electronic identification or by presenting an official photographic identity document.

d) A user may have read-only access or read and write access to a system
Depending on the system and the user's role or task, the user may have read-only access or read and write access to the system. For example, all members of the Aalto community have

by default read-only access to materials intended for the Aalto community. If a user's tasks so require, they can be given write access, enabling them to create and edit content on Aalto.fi.

When usernames and passwords are provided electronically, an audit trail must always be created, and strong encryption is also obligatory.

Some shared usernames and group accounts may also be in use at Aalto University. In these cases, access rights are connected to the username or account in question. Read more in Section 2.4 on jointly used usernames.

2.2 Administrator usernames

System administrators use separate, personal usernames intended for this purpose. Usernames equipped with administrator rights may not be used for other daily work or private purposes, such as email or browsing the Internet.

Administrator rights are granted to those who need them. A Head of Services, or someone else they have authorised, decides on the granting of administrator rights to designated persons. Administrator rights are granted to separate usernames that personally belong to each administrator.

IT Services maintains a list of administrator rights and administrators. The Head of Services must ensure that all persons with administrator rights have been entered into the list, and that the list is up to date. The person in charge and IT Services review administrator rights according to the university's internal annual schedule.

For protected resources, IT Services must define the roles that are necessary for the administration of the resource in question.

2.3 Technical and service usernames

Technical and service usernames have an owner who is responsible for their documentation. The owner is named in the documentation of the information system.

2.4 Jointly used usernames

Jointly used usernames refer to group usernames and shared usernames. The confidentiality of jointly used usernames must be protected by changing the password regularly and whenever necessary. The Head of Services, or another person appointed by them, works with IT Services to review all jointly used usernames in their area of responsibility according to the university's annual schedule.

2.4.1 Shared usernames

The sharing of usernames is only permitted in exceptional circumstances and on justifiable grounds, for example, for research purposes. The asset owner (e.g. an information system) decides on the use of shared usernames.

The processing of personal data using a shared username is prohibited. ‘Personal data’ refers to any data that permits or may permit a person to be identified. Examples of personal data include name, IP address and vehicle registration number. ‘Processing’ for example includes the collection and disclosure of personal data.

When confidential data is processed, it is important to ensure that everyone who uses the shared username has a need and a right to access the data.

Every person who uses a shared username is, for their own part, responsible for the actions they take while using the username. In the case of shared usernames, particularly good care must be taken of high password quality and of changing the password regularly, to ensure information security. Read more in the password guidelines.

2.4.2 Group usernames

Group usernames are intended for temporary use and only permitted for special purposes. Group usernames, used by several people, may be granted for special purposes, for instance, for the participants of a course held in a computer classroom.

The person requesting a group username may not reveal it to anyone except the people for whom it was requested, such as the course participants. The Head of Services authorizes the use of the group username. The group username may only be used for the purpose for which it was granted.

Group usernames are temporary. When a group username is created, it must be given a period of validity. The username will expire after this time.

Every user of the group username is responsible for their actions while using it. Confidential information and personal data may not be processed using the group username. When using group usernames, pay particular attention to the section ‘password use’ above.

3 Granting and management of access rights

a) Access is based on a written contract and on the user’s commitment to the information security and data protection rules

Access rights are based on the service relationship that exists between a person and Aalto University, or another written contract between a person and Aalto University. The person who has been granted access has to sign a written commitment to Aalto University's data protection and information security policies and rules, orders and instructions. The person commits to keep their username and password secret and to not misuse them.

b) Access is based on a person's role (role-based access control)
Access rights are grouped into roles and groups, and a person may have several roles and groups. By default, when a person belongs to a specific group, such as students, access to the systems and data belonging to the group is opened to him or her. These roles and groups, and the access rights associated with them, must be described and the procedure must be approved by the Head of Services. Should the person's role change, access rights to both physical facilities and systems must be edited accordingly.

c) Decisions on access rights are made by the Head of Services, but requirements arising from different sources must be taken into account
The Head of Services decides on the granting of access and the use of a secure login method (multi-factor authentication, MFA). When access rights are granted, account must be taken of statutory and contractual requirements, requirements related to the activities of Aalto University, and particularly the need to protect personal data and assets of Aalto University (e.g. its trade secrets).

d) Access rights are granted primarily through the access rights management system
As a rule, access rights are granted, edited and revoked through the access rights management system. In situations where the access rights management system needs to be bypassed, see the principles described in the first section of this document.

- If the Head of Services does not manage the access rights of a system, the person must appoint another person to this task.
- An up-to-date list is kept of a system's users.
- Users have only the rights they need to perform their duties. Access is limited to the networks, data and systems related to their own work, studies or assignments.
- When access rights are granted, steps must be taken to reliably verify that the recipient is a staff member or otherwise authorised to have access.
- Written instructions on how to process and grant access rights have been drawn up for each system.

- There is a clear and effective way of notifying the parties concerned immediately of any changes in the staff, the student body and among the staff of the university's partners, and an effective way of making the necessary changes.
- Changes in access rights are reflected in both physical and logical access rights and use.
- Access rights are regularly reviewed.
- There is a register of the authorised staff members of partners and other third parties.
- Logs are kept of all access rights that are granted.

4 Creation and granting of usernames and access rights

4.1 Phase 1: Creation of usernames

Before a user can be registered and a username created, the identity of the user must be verified using a strong identification method (electronic identification or an official photographic identity document). User registration and a username alone do not provide access to networks and online services. The person who has been granted access has to sign a written commitment to Aalto University's data protection and information security policies and rules, orders and instructions.

4.2 Phase 2: Granting of access rights

A registered user (username) is allowed access only to the networks and online services to which they have been expressly granted access rights. In principle, access rights are granted on the basis of a role, if the person has a role at Aalto University. However, the user's need to access and use information is taken into account when granting access rights.

For employees, the right of access to Aalto University's information systems enters into force on the day the employment relationship begins. For justified reasons, the right of use may begin 7 days before the employment relationship.

Students are granted access to those Aalto University information systems they need for studying when their right to study is in force.

Other parties are granted access rights on a case-by-case basis, taking into account their need to access and use information. This applies, for example, to persons working on commission.

5 Revocation and editing of access rights and usernames

The *right of access* to an information system is revoked when:

a) the person is no longer a member of the Aalto University community;

b) the right of access has been granted for a fixed term and it expires;
c) the role of the person changes in such a way that their right to access the information system is no longer justified; or
d) it is necessary because information security has been compromised, for example, to investigate an IT offence or to protect data and information.

A *username* is revoked when:
a) access rights, to which the username is connected, are revoked;
b) the username is no longer needed; or
c) there are justifiable grounds to suspect that the username has been misused and information security has been compromised.

When access rights to basic IT services expire, the user's email address will also expire and no longer receive new messages. Read more in the email and instant messaging policy for students, and the email and instant messaging policy for Aalto University units and staff.

5.1 Reassessment and editing of access rights

The Head of Services works with IT Services according to the annual clock of the Information Security Management System (ISMS), to regularly reassess access rights and to delete expired and unnecessary access rights. Any necessary changes to or revocation of access rights are handled primarily by the person's supervisor, and secondarily by the Head of Services. They perform regular reviews of the appropriateness of access rights according to the annual schedule.

If a licence or user fee is paid for each right of access to the system, the Head of Services (or a person authorised by them) must regularly ensure that only persons who need licences for work or studies have a licence for that system.

5.2 Practical situations, staff

A staff member's right of access to Aalto University information systems ends eight days after their employment relationship ends (date of expiry of the contract). Hourly teachers' access rights will expire at the end of the semester during which their hourly teaching appointment ends.

A user must ask IT Services to terminate their username if the user will not use it during a long absence, for example. If an employee ceases to perform their duties before the employment relationship actually ends (for example, due to a leave of absence), the unit may ask IT Services to terminate the username when the person stops working. If the person has agreed to continue performing certain

tasks (e.g. study guidance) after the employment relationship ends, the unit may notify IT Services of the extension of the person's access rights without an employment relationship. In such cases, however, it may be necessary to re-examine the scope of access rights, as the person's status at Aalto University has changed.

5.3 Practical situations, students

A student's right of access remains valid for 4 months from the date of graduation, and is revoked after this date.

After this period, the student may apply for an extension for very compelling reasons only. The student should send the request for extension to their own Office of Studies and Registrar. After a certain period, the access right cannot be reactivated.

6 User's responsibilities

6.1 Sharing of usernames and passwords

Usernames and passwords are personal and confidential. They may not be disclosed to anyone else. The user is responsible for all actions taken and data saved using their username and password.

6.2 Loss of confidentiality

The user must immediately inform Aalto University's information security team if the user suspects that their username and password have fallen into someone else's hands.