Amsterdam University of Applied Sciences

Authorisation policy

Adopted by the Executive Board as decision no. 2021hcb061 on 02 March 2021.

Creating Tomorrow

Contents

References

[GDPR]	General Data Protection Regulation https://www.privacy-regulation.eu/nl/index.htm
[BOM]	Basic set of operational information security measures Not yet published.
[ClassRL]	Classification guideline for information and information systems Not yet published.
[EIDAS]	Regulation (EU) no. 910/2014 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=NL
[IB]	*Informatiebeveiligingsbeleid Universiteit van Amsterdam, v1.2, 28-07-2018*
[ISO27001]	NEN-EN-ISO/IEC 27001:2017 Information Technology – Security techniques – Information security management systems
[ISO29115]	NEN-EN-ISO/IEC 29115:2011 Information Technology – Security techniques – Entity authentication assurance framework
[RLWW]	Password and means of authentication guideline Not yet published.
[RvVG]	Rules for responsible use of ICT facilities HvA NL: https://www.hva.nl/praktisch/algemeen/hva-breed/its-si/ict-gedragsregels/ict-gedragsregels.html HvA ENG: https://www.amsterdamuas.com/practical-matters/general/auas/its-si/ict-code-of-conduct/ict-code-of-conduct.html
[Surf IB]	SURF Standards Framework on Information Security https://www.surf.nl/informatiebeveiliging

1 Introduction

For the Amsterdam University of Applied Sciences (AUAS) to function properly, it is vital that information be handled with the greatest of care. Students, employees, and other relevant stakeholders should feel safe in the knowledge that information is accessible only to authorised users. Users could be an organisation, department, individual, technical system or process.

Whether a user is actually correctly authorised is determined according to the following key terms:

1. **Means of identification**: a user has a unique means of identification that refers to the user, such as a name, citizen service number, email, account name, or pass. Users may possess multiple means of identification;
2. **Identification**: a user discloses his/her identity by showing a means of identification;
3. **Authentication**: verification of whether a user really does possess the means of identification being used to disclose his/her identity;
4. **Authorisation**: the granting of rights to a user, such as the right to create, read, write, edit and delete data or to carry out a process.

The authorisation policy is an important element in the protection of personal and other data of the university and contains guidelines on the application of the above key terms.

2 Target Group

This policy applies to anyone in the AUAS with responsibility relating to authorising users. Examples of such individuals are owners[1], such as process owners, system owners, application owners and project owners. They bear responsibility for properly protecting information (and for the introduction of such protection), which includes authorisation.

Functional managers have an important role in setting up and maintaining authorisations and in periodically validating them, and reporting on them to the owner.

The policy does not extend to individual users who grant others rights to view or collaborate on a document. These responsibilities are set down in the 'Rules for responsible use of ICT facilities' [RvVG].

3 Scope

The authorisation policy relates to the protection of all information at the AUAS and includes every operation in which information is processed, be it physically or digitally. Authorisation applies to every information-processing operation, system, application, storage medium and location.

The authorisation policy is a detailed version of part of the **information security policy** [IB] and meets **standard ISO 27001:2017** [ISO27001], clause A.9, 'Access security', as well as the sub-clauses and the SURF Standards Framework on Information Security [Surf IB], Cluster 5 'Confidentiality and Integrity', VI.05 'Rights of access'.

The authorisation policy provides guidelines on how to deal with authorisations. Authorisation methods may require varying numbers of steps, depending on the sensitivity of the information being

[1] Ownership in this context is not set down in law, but usually rests with the manager of the process that uses the system or data for which access is required (in the manager's own faculty or unit).

processed. How sensitive information is classified is set out in the '**Classification guideline for information and information systems**' [ClassRL]. The measures that should be applied, depending on the information classification, are set out in the '**Basic set of operational information security measures**' [BOM].

4 Purpose

The purpose of authorisation is to grant appropriate rights to a particular user. Issuing only the rights that are needed for a function to be carried out means that information is protected against breaches of confidentiality, integrity and availability, and that the AUAS and its associates are protected against possible harm.

The authorisation policy describes the starting points and requirements relating to the identification, authentication and authorisation of AUAS users. This means the authorisation policy is an important organisational measure for granting authorisations and for complying with relevant legislation, such as the General Data Protection Regulation (GDPR). The policy requirements should be applied to every information system (with the definition of 'information system' being taken broadly), such as systems, applications and data carriers, as well as physical data carriers and locations where information is found.

5 Starting points

The following policy starting points apply:

1. Each user must be checked to see whether he/she has the right to access information. The process owner has primary responsibility in this regard.
2. The owner of a system or application that processes information is responsible for the effective structure and organisation of the authorisation procedure.
3. Before a user is granted access to information, he/she should be correctly identified and then given a physical and/or digital means of identification.
4. Access to information and information systems is granted for the following reasons:
    a) The 'need-to-know' principle: access is granted only to the extent that is needed for the work in question to be carried out.
    b) The purpose limitation principle: access is granted only to the data for which a justified purpose exists; data not related or relevant to the purpose will remain protected. If the purpose changes or is modified, a new request for access must be made.
    c) It is the classification of the information that determines what protection measures are appropriate.
5. In the case of more complex systems, the person responsible for the data is not the same person as the system owner. Responsibility for a system generally rests with a central unit, while responsibility for data lies with a degree programme or faculty. Responsible officers are referred to in this policy as process owners. Process owners are responsible for the data in their systems. System owners are responsible for the authorisation policy of their systems and for coordinating activities with process owners.

6 Roles and responsibilities

Key roles among the Executive Staff

6.1 Chief Information Security Officer (CISO)

The CISO is responsible for policy, frameworks and guidelines relating to information security and for verifying compliance with these. This means the CISO is also responsible for upholding the authorisation policy.

The CISO has the task of verifying whether the periodic checks of authorisations by system owners are carried out correctly.

Together with the internal Audit department, the CISO ensures that the authorisation process for operational processes is audited.

Decentralised roles

6.2 Process owner, business owner

Process owners are responsible for correctly protecting data in systems and applications that support the process in question and, in accordance with this policy, have the responsibility of determining which users are entitled to access information. In exercising their responsibility for ensuring proper protection, process owners are supported by the system owner and/or application owner.

Another term for process owner is ‘business owner’.

6.3 System owner, application owner, product owner

System owners support process owners by properly structuring and organising the authorisation procedure of the system, and coordinate activities with process owners.

System owners are responsible for periodic checks of user authorisations and report on them to process owners and the FISO.

Other terms for system owner are ‘application owner’ or ‘product owner’.

6.4 Project owner

Owners of AUAS projects are responsible for ensuring that the correct authorisations are set up, modified, or deleted when structuring or altering information-processing systems.

6.5 Functional manager

Functional managers contribute their knowledge about information, systems and processes. Functional managers support system owners when carrying out the authorisation process, their periodic checks, and when reporting on the results of these checks.

6.6 (Faculty) Information Security Officer ((F)ISO)

The FISO has the task of verifying whether the periodic checks of authorisations by system owners are carried out correctly, and of reporting on these checks to the CISO.

7 Policy implementation

The authorisation policy is set by the Executive Board. The CISO is responsible for maintaining the document content and for the four-yearly periodic reviews.

Once this policy document has been adopted, it will be implemented as follows:

- The CISO publishes the policy and brings it to the notice of everyone to whom it applies.
- The CISO is responsible for drawing up the 'Password and means of authentication guideline' [RLWW], which specifies the requirements on passwords and the use of means of authentication for the various levels of confidentiality.
- System owners implement or improve the authorisation procedure for the systems under their responsibility.
- Together with the internal audit department, the CISO initiates a programme for monitoring compliance using periodic random internal audits.

8 Identification

Identification is the disclosure of the identity of a user. A user can be an organisation, department, person, technical system, or process. Users must have a means of identification to be able to perform actions in the physical and digital worlds. A means of identification can be personal or non-personal. Depending on the type of work due to be carried out, a certain level of confidentiality of the identification process may be required.

This chapter sets out the requirements in greater detail.

8.1 Digital means of identification

A digital means of identification serves to identify a user in the digital world. Examples of digital means of identification are a social media account, an account with a username and password, an email address, a digital certificate, etc.
Policy guidelines for digital means of identification are:

1. At the start of a user's relationship with the AUAS, the user is allocated a digital means of identification.
2. This is recorded in a source system. Different source systems may be used for different groups of people.
3. Upon termination of a user's relationship with the AUAS, the digital means of identification is immediately deactivated, an operation carried out from the source system.
4. Digital means of identification are unique and linked to a single user; they are not transferable and may not be reused for other users.
5. A user may be allocated more than one digital means of identification to facilitate the segregation of functions.
6. There is a watertight register of users linked to digital means of identification.
7. Administrative accounts are only issued in a particular name.

8.2 Non-personal means of identification

Non-personal means of identification are those not linked to a natural person. Examples include: main administrative or root accounts, system accounts, functional or group accounts, digital key or certificate. Non-personal means of identification may not generally be used by people, only by systems.

Policy guidelines for non-personal means of identification are:

1. Main administrative accounts are blocked, as standard. The associated password is stored in a physical or digital safe.
2. System accounts are necessary for technical services that have to identify themselves to other technical services. Users and administrators are not permitted to use these accounts.
3. The use of functional accounts[2] or group accounts is forbidden, unless implementation is technically impossible[3].
4. In exceptional cases where an account is used by one or more users/administrators:
    a) There is a watertight register of users with access to the account.
    b) If any of the users/administrators leaves the AUAS or changes position, his/her identification data should be changed immediately.
5. A secure provision has been arranged so that in the event of an emergency (where the administrator is unexpectedly unreachable and immediate action is needed), access can be granted to an administrator.
6. Access to digital safes is by name and a two-factor authentication is used.

8.3 Identification of reliability levels

The way in which a user is identified determines the degree of certainty of the user's claimed identity. The following levels apply:

Level 0: no verification

The identity of the user is not subject to any verification. These users may consult public sources without disclosing their identity.

Level 1: self-verification

This level offers little or no certainty with regard to the identity claimed by the user. When registering, identifying features of the individual are accepted without any further verification. At the AUAS, this applies to visitors to conferences, for example. Registering using a social media account is another example of identification at this level.

Level 2: verification by invitation

Identification at level 2 applies whenever a user is granted a means of identification at the request of an employee. The issuing of a visitor pass or guest account via the self-service functionality is an example of this. The employee who makes such a request is responsible for establishing the identity of the user.

Level 3: verification using reliable source

At this level, verification of the identity claimed by the user is carried out during the registration process using a means of identification from a reliable source. The source could be a reliable internal

[2] A functional account is one used by a person but which is not visibly personal.
[3] This could be because the supplier or implementation does not (yet) meet this guideline, for example.

system, such as the HR system or the ICT identity management system. The use of a username and password issued by the AUAS comes under this level.

The source could also be an external entity, for example involving a check (possibly using a third party) against the Municipal Records Database (GBA). This level is used for identifying students. Student data are checked against the GBA, via Studielink.

Level 4: verification using an official document

Identities at this level must actually be established by comparing a valid official document in the user's possession with the records in a key register. Physical presence is not required in the registration process, and the checks may be outsourced to a reliable contracted third party or carried out remotely.

Level 5: face-to-face verification

At this level, users must present themselves in person at least once in order for their identity to be verified; this is supplementary to the method used at level 4. This level offers a higher degree of certainty about the identity of the user. The identification of permanent employees, whose passports are checked at the time of their appointment, takes place at this level.

Identification policy guidelines

Identification policy guidelines are:

1. For identification at reliability levels 1 and 2, the end-date of the validity of the means of identification should always be recorded.
2. The classification of the information[4] to which access is to be granted determines the identification level to be used for such access. Table 1 shows how the reliability levels correspond to the classification levels in the classification guideline [ClassRL].
3. The AUAS is bound by the European eIDAS [EIDAS] regulation on electronic identification. Table 1 shows how the identification reliability levels correspond to the levels in the eIDAS regulation.

Identification of reliability level	Classification level	eIDAS level
Level 0	-	-
Level 1	Low	-
Level 2	Low	-
Level 3	Low / Standard	eIDAS Low
Level 4	Medium / Sensitive	eIDAS Substantial
Level 5	High / Critical	eIDAS High

Table 1: Relationship between identification reliability levels

9 Authentication

Authentication is the process used for checking whether a user really is who he/she claims to be. A check is carried out on whether a means of identification presented includes the security features registered in the system. The authenticity of the means of identification is validated. This chapter sets out the requirements in greater detail.

[4] This classification is a compulsory aspect and takes place in an IB&P workshop.

9.1 Authentication methods

There are various authentication methods. The following levels apply:

Level 0: No authentication required

No authentication takes place at this level; users' identities do not need to be known before they gain access. An example of this includes viewing information that is publicly available, such as the website.

Level 1: One-factor authentication

One-factor authentication is a check on a user's identity based on one feature, such as a PIN code, username and password, or a unique code received by the user from a trusted party.

Level 2: Two-factor authentication

Two-factor authentication is a check on a user's identity in accordance with level 1, but with an additional second feature, such as a hard token (a pass or hardware key), soft token (a one-off code sent to the user or a code generated by an authentication app) or biometric identification. See 'Password and means of authentication guideline' [RLWW] for the correct applications.

Level 3: Multi-factor authentication

In the case of multi-factor authentication, there should be a second factor present of a sufficiently strong level, or an extra authentication factor should be added. See 'Password and means of authentication guideline' [RLWW] for the correct applications.

Policy guidelines

Policy guidelines for authentication methods are:

1. If an information system is unable to make a distinction between higher and lower classified information, then the authentication required for the higher level should be applied.
2. If two-factor authentication is used, then both means of authentication should be linked to the user. The means of authentication should be designed in a way that they can only be used under the control of the user. There must be no possibility of their being used by another person, accidentally or otherwise.
3. The AUAS is seeking to use Single sign-on (SSO) across the board[5].
4. The classification of the information to which access is to be granted determines the authentication level to be used for such access. Table 2 shows how the reliability levels correspond to the classification levels in the classification guideline [ClassRL].
5. The AUAS is bound by the European eIDAS [EIDAS] regulation on electronic identification. Table 2 shows how the authentication reliability levels correspond to the reliability levels in the eIDAS regulation.

[5] Single sign-on enables users to log in once, after which they are granted automatic access to multiple applications and sources in the network.

Authentication of reliability level	Classification level	eIDAS level
Level 0	-	-
Level 1	Low / Standard	eIDAS Low
Level 2	Medium / Sensitive	eIDAS Substantial
Level 3	High / Critical	eIDAS High

Table 2: Relationship between authentication reliability levels

9.2 External authentication

The authentication process may be outsourced to a trusted third party - this is sometimes referred to as federated authentication[6].

Policy guidelines for federated authentication are:

1. Federated authentication is permitted with a trusted third party with whom contractual agreements have been made on the reliability levels in force at the AUAS (see Appendix A).
2. The AUAS may make services available that use federated authentication.
3. The AUAS may purchase services by third parties who use federated authentication.

9.3 Distribution

The distribution of means of authentication should be done securely.

Policy guidelines for distribution are:

1. The distribution of means of authentication through a non-secure channel such as email, text message, or an employee, is only permitted for one-off codes such as a temporary password or activation code.
2. The distribution of means of authentication that have been in use for some time is permitted only through a secure channel.

Examples of secure distribution are:

- Users receive a message on an internal or external email address that they have provided themselves, containing a link with a one-off activation code. They can then use this link to create a password in a secure environment.
- The user goes to the ICT service desk and is given a means of hardware authentication from an employee there, after a face-to-face check.

Examples of non-secure distribution are:

- Automatically sending a username and password by email (internal or external).
- One employee passing on a (hardware) means of authentication to another.

9.4 Logging and monitoring

For the sake of transparency, traceability and audits, authentications should be recorded.

Policy guidelines for logging and monitoring authentication are:

1. Every authentication should be registered for possible subsequent checks.

[6] An example is that of SURF, with the SURFconext service. Using a social media account, for example, is not federated authentication, because there are no agreements on checks on identity details.

2. For each authentication, the following must be recorded: the means of identification presented, the time at which this occurred, authentication method, identification of the validating entity, and the result of the authentication.
3. The owner is responsible for periodically checking the logging for any unusual behaviour.
4. Attempts at unauthorised entry should be reported to the Computer Emergency Response Team (CERT).

9.5 Password policy

Passwords should be sufficiently strong. Password requirements are described in the 'Password and means of authentication guideline' [RLWW].

Policy guidelines for passwords are:

1. Passwords should not be easy to guess.
2. Password storage must be encrypted.
3. Passwords may only be transported if they are encrypted.

10 Authorisation

Authorisation is the process in which a user is granted the right of access to information or information-processing systems. Authorisations are primarily granted by the relevant process owner. This chapter sets out authorisation requirements in greater detail.

10.1 Authorisation procedure

The granting of rights to users is conducted through a formal authorisation process, in order to ensure that rights are allocated appropriately. A sample authorisation process is shown in Bijlage B.

Policy guidelines for the authorisation procedure are:

1. Rights are granted to users only through a formal authorisation procedure.
2. Functions are clearly defined in any authorisation procedure, with the involvement of at least the following roles:
   a) **Applicant**: requests authorisation and changes to authorisations for a user[7].
   b) **System owner**: sets down the authorisation matrix[8].
   c) **Functional management**: checks, on behalf of the owner, the application and validates it against the authorisation matrix and is in charge of the authorisation procedures.
   d) **Technical management**: implements authorisation changes that have been approved. This role may also be carried out by the functional manager.
3. An authorisation procedure involves checks on whether the application in question has been submitted on time, whether it is complete and clear, and whether the applicant is empowered to make an application.
4. Users may not apply for their own authorisations because of the requirement that functions be segregated.
5. An authorisation procedure must be followed in the case of applications for new authorisations, for modifications to authorisations and for the revocation of authorisations.
6. Applicants have primarily responsibility for notifying functional management of any authorisations that have been revoked.

[7] Applicants are typically supervisors or process owners.
[8] See §10.2 for definition.

7. A user's authorisations are revoked if:
    a. The relationship between the user and the AUAS comes to an end;
    b. The user changes job or role to one that does not confer the right to access information;
    c. They have been absent for longer than two months;
    d. They have been suspended or dishonourably dismissed;
8. A user's authorisations may be revoked by order of the EB if:
    a. The user acts in breach of the 'Rules for responsible use of ICT facilities'[9].
9. Authorisations that have been revoked may only be reactivated with the explicit approval of the process owner.
10. There should be a procedure at the AUAS where system owners receive a signal if there are any relevant changes relating to a user, as described under points 7, 8 and 9.

A more specific version of this procedure will be needed for complex systems.

10.2 Authorisations, roles and rights

Granting access to information involves the conferring of rights or powers. These could be:

- Creating: confers the right to create new information.
- Reading: confers the right to view or read information.
- Modifying: confers the right to modify information.
- Deleting: confers the right to permanently delete information.
- Copying: confers the right to make a copy of information.
- Execution: confers the right to execute code.

Rights are linked to roles, and roles are allocated to users. The registration of the link between rights and roles is known as an **authorisation matrix**.

Policy guidelines for authorisations are:

1. Information may not be accessed or used without authorisation. The only exception to this is information that is covered by an open-access policy.[10]
2. Access to information is granted primarily on the grounds of organisational roles to which rights are linked according to the authorisation matrix.
3. Users only gain access to information that they actually need in the context of their role.
4. Access that has been granted for specific information does not imply access rights to any other information.
5. Technical access to information for the operations of the system is authorised using system accounts specially created for the purpose, and not user accounts.
6. The allocation and use of special powers that enable users to circumvent the usual security measures (to carry out specific administrative activities, for example) should be limited.

10.3 Segregation of functions

No conflicting roles should be allocated to one person that could lead to harm to any individual or the AUAS, such as the opportunity to commit fraud.

Policy guidelines for segregation of functions are:

1. Process owners are responsible for identifying the roles in the process in which functions need to be segregated.
2. Conflicting roles are indicated as such in the authorisation matrix.

[9] Rules on this are set out in the 'Rules for responsible use of ICT facilities' [RvVG], Article 10.1.
[10] Examples include the public website and certain research results.

10.4 Logging and monitoring

For the sake of transparency, traceability and audits, authorisations should be recorded.

Policy guidelines for logging and monitoring authorisation are:

1. Authorisations allocated to users should be registered for possible subsequent checks.
2. Modifications to authorisations allocated to users should be registered for possible subsequent checks.
3. For each modification to an authentication, the following must be recorded: the user who makes the modification, the time at which this is done, the user whose authorisation has been modified, and the newly allocated authorisation.
4. The system owner is responsible for periodically checking the logging for any unusual behaviour.
5. Suspected misuse should be reported to the Computer Emergency Response Team (CERT).

11 Compliance

11.1 Periodic checks

It is important to carry out periodic checks on whether the allocated authorisations are still correct, as too many allocated rights could undermine the principle of functional segregation and lead to a greater risk of harm to individuals or to the AUAS.

Policy guidelines for periodic checks are:

1. The system owner[11] is responsible for periodic checks of the correct link between users and their roles.
2. The system owner is responsible for separate periodic checks of the users with administrative powers.
3. The system owner is responsible for periodic checks of the link between roles and the rights allocated to the roles. These checks typically take place less frequently than do the periodic authorisation checks.
4. Any errors detected are rectified as quickly as possible.
5. The frequency of checks depends on the classification of the system, as follows:

Classification	Regular users	Special powers	Roles and rights
Standard / Low	twice a year	twice a year	once every two years
Sensitive / Medium	twice a year	twice a year	once every two years
Critical / High	four times a year	four times a year	once a year

[11] This also applies to outsourced systems, applications and in the cloud.

11.2 Periodic reports

Authorisations are a crucial part of the security of the information at AUAS, which is why a second line of defence is needed.

Policy guidelines for periodic reports are:

1. Periodically, at least twice a year, the (F)ISO receives reports on the authorisation checks from the all the system owners that are classified as Sensitive or Critical for Integrity and Confidentiality.
2. The CISO ensures that periodic authorisation checks are carried out periodically and are of sufficient quality.

11.3 Audits

Authorisations of systems that support operational processes are a crucial part of the security of the information at AUAS, which is why a third line of defence is needed.

Policy guidelines for audits are:

1. Periodically, at least once a year, an external party conducts an audit of the authorisation process for financial processes.
2. Together with the internal Audit department, the CISO ensures that the authorisation process for operational processes is audited.

Appendix A Level of Assurance

This appendix contains a summary of the requirements set out in Chapters 8 (Identification) and 9 (Authentication).

The chain of authorisation is only as strong as its weakest link. With this in mind, the different parts of the chain must always have the same level of strength at the very least. The table in this appendix shows the various levels and the comparable levels of strength between them. The lowest level of strength in the chain as a whole determines the Level of Assurance (LoA). Also see [ISO 29115]. The Level of Assurance depends on:

- the degree of reliability of the identification process in which a user is identified;
- the degree of reliability of the authentication process (involving no authentication or one-factor or two-factor authentication);
- the way in which means of identification and authentication and information elements are distributed;
- the degree of reliability of the means of authentication (not specified in the table).

LoA level [1]	eIdas level [2]	Classification level [3]	Identification level [4]	Authentication level [5]	Distribution of means [6]
LoA 0		-	Level 0: none	Level 0: none	-
		Low	Level 1: self-verification		Via an unsecured channel
LoA 1		Low	Level 2: by invitation		Via a secure channel
LoA 2	Low	Low / Standard	Level 3: via a trusted source	Level 1: One-factor authentication	Via a secure channel
LoA 3	Substantial	Medium /Sensitive	Level 4: via an official document	Level 2: Two-factor authentication	Via a secure channel
LoA 4	High	High / Critical	Level 5: face-to-face	Level 3: Multi-factor authentication	Via a secure channel

[1] Level of Assurance
[2] eIdas [EIDAS]
[3] See Classification Guidelines [ClassRL]
[4] See chapter **8**
[5] See chapter **9**
[6] See chapter **9**

Appendix B Example of authorisation process