Amsterdam University of Applied Sciences

Classification guidelines

Information and information systems

Adopted by decision No. 2021hcb061 of the Executive Board on 02-03-2021.

Creating Tomorrow

Contents

References

[BIHU]	AUAS-UvA Information Security Baseline, v1.0, 13-05-2015
[BOM]	Basic set of operational measures concerning information security (Basisset operationele maatregelen informatiebeveiliging) Not yet published.
[CMDB]	Central database used to store system characteristics. This may be a central system (at ICTS) or a separate document for a faculty.
[IB]	Amsterdam University of Applied Sciences Information Security Policy,23-10-2018
[IB&P]	Information Security & Privacy Risk Assessment: • IB&P risk assessment for teaching, education and operational management • IB&P risk assessment for research(Not yet published).
[ISO27001]	NEN-EN-ISO/IEC 27001:2017 Information Technology - Security techniques - Information security management systems

1 Introduction

Handling and managing information is crucial to the proper functioning of the Amsterdam University of Applied Sciences (AUAS). Students and staff must be able to rely on information being available when and where it is needed, as well as that it is correct and accurate and only accessible to authorised persons.

It makes sense to differentiate the various levels of information protection. For example, not all information is confidential and it would not be user friendly to subject non-confidential data to as stringent protection as for highly confidential information. This requires a degree of proportionality, including for the purposes of ensuring efficient use of the available funding. Classification of information is tool that can be used to establish proportionality between the value of the data and the cost of measures to be taken to ensure an adequate level of protection.

This document outlines the classification method used to classify data and information systems according to the quality aspects of Availability, Integrity and Confidentiality, on the basis of which the appropriate level of protection is determined. Selection of the technical and organisational security measures required for the adequate protection of information will subsequently take place based on the level of protection determined.

2 Target group

The primary target group for these guidelines is everyone at the AUAS who has a responsibility in relation to the processing of data and therefore its protection, such as process owners, data owners, system owners, application owners and project owners, who are responsible for the introduction of adequate protection of information.

The secondary target group is anyone who is involved in implementing changes to information processing, information handling processes and systems. This group plays a role in the correct classification of the information and thus in determining the appropriate level of protection.

3 Scope

The classification guidelines apply to all information of the AUAS, regardless of the medium in which this information is stored and regardless of its presentation, and to the systems in which this information is stored (information systems).

The classification guidelines are an elaboration of a part of the information security policy[1] and implement the standard ISO 27001, clause 8.2.1.

Classification is not a one-off activity, but rather is a cycle that must be repeated on the basis of new insights (e.g. as a result of actual incidents) or following the introduction or modifications of functionality, which may lead to modification of classification and security measures.

The elaboration of this policy into a set of instructions and a practical guide for carrying out and documenting the classification of information and information systems is set out in '**IB&P Risk Assessment**' [IB&P].

The description of the technical and organisational security measures to be selected on the basis of the outcome of the classification is not part of these guidelines. Measures are described at a high level of

[1] Please see Information Security Policy [IB], Appendix B.

abstraction in the Information Security Baseline for Higher Education (Baseline Informatiebeveiliging Hoger Onderwijs, [BIHU]). For the purposes of implementation, a basic set of operational measures is required, corresponding to the different levels of protection[2]. This basic set of operational measures is outlined specifically for the AUAS in the 'Basic set of operational measures concerning information security' [BOM].

4 Purpose

Classification of information contributes to a safe learning and working environment, to compliance with legislation such as the GDPR, and therefore to the image of the AUAS Similarly, classification of information helps select the measures that need to be taken in order to adequately protect information, ensure its integrity and optimise its availability, as well as increases the alertness of the organisation in relation to the value of information and security risks.

The aim of the classification guidelines is to set out a clear method of classifying information based on the quality aspects of Availability, Integrity and Confidentiality in order to be able to determine the appropriate level of protection on that basis. Based on the outcome, namely the required level of protection, the corresponding security measures can be selected for the adequate protection of information, using the 'Basic set of operational measures concerning information security' [BOM].

5 Key principles

The following basic policy principles apply:

1. Data, processes, applications and systems have a business owner. With regard to the overarching corporate systems of the AUAS, officers have been appointed who carry out the role of system owner.
2. The delegated owner determines the classification and therefore the required level of protection.
3. The CISO, in consultation with the user organisation and ICTS, determines what security measures are appropriate for the protection level.
4. When processing information, the classification level of the system or application in which certain information is used may be different from what would be expected based on the classification of the information (alone). Rather, the context is relevant to the classification.
5. The aim is to achieve a responsible classification level that is as 'low' as possible; unnecessarily high classification leads to unnecessary measures and costs.
6. Where a risk assessment shows that additional measures are necessary, these must be taken. The standard security measures prescribed for the level of protection are not an automatic guarantee of adequacy.

6 Roles and responsibilities

Central roles within the Executive Staff

[2] Please see H8.1.

6.1 Chief Information Security Officer (CISO)

The CISO is responsible for policy, frameworks and guidelines in the field of information security. The CISO determines the method of information classification and contributes to the determination of the information classification in consultation with the owner and approves the information classification.

The CISO is responsible for the creation, maintenance and monitoring of the procedure and instructions for the IB&P risk assessment [IB&P] for teaching, education, research and operational management.

Decentralised roles

6.2 Owner

The owner, such as the process owner, data owner, system owner, application owner, product owner and project owner, has final responsibility for the implementation and the outcome of the classification (please also see key principle 1). The owner decides on functionality and changes therein, performs the information classification on that basis and bears the costs related to information security. The owner is responsible for documenting the classification of information and obtaining approval from the CISO. The owner is also responsible for implementing the required security measures.

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

The (Faculty) Information Security Officer is able to contribute to determining the information classification in consultation with the owner, and approving the information classification, on behalf of the CISO.

The (F)ISO shall keep a record of the proper classification of systems within its domain in a [CMDB].

6.4 System Administrator

The systems administrator provides substantive knowledge of information, systems and processes during the information classification process.

7 Policy implementation

The classification guidelines will be adopted by the Executive Board. The CISO will be responsible for maintaining the content of the document and its periodic review every 4 years.

From the moment of adoption of these guidelines, information classification of information and information systems will be applied using the IB&P Risk Assessment [IB&P] for teaching, education, research and operational management. A procedure/manual/set of instructions will be developed for each sub-area under the responsibility of the CISO and the Data Protection Officer.

The (F)ISO of the faculties or departments will keep a record of the appropriate classification of information and information systems within their domain in a [CMDB].

The CISO will be able to determine whether information and information-processing systems have been classified correctly, as well as whether the correct protective measures have been taken effectively, by way of audits.

8 Classification methodology

8.1 Terminology

This section defines the terms and classifications used in the classification methodology.

The classification uses the general concept of ‘damage’, which refers to damage to the interests of the AUAS, its employees, students or customers.

Availability

Availability is understood to mean: ensuring that authorised users have timely access to information and related facilities at the right times.

Aspects that determine availability include reliable power supply, proper fire safety, the presence of an up-to-date continuity plan, reliable reserve copies and the lack of ‘single points of failure’. Other key aspects are the existence of sufficient access opportunities for the intended number of simultaneous users and protection against so-called 'Cyber threats'.

In terms of availability, the following classes are distinguished:

Class	Description
Low	Overall loss or unavailability of this information for **more than 2 days** will cause some noticeable (measurable) damage.
Medium	Overall loss or unavailability of this information for **one or two days** can cause serious (in)direct damage.
High	Overall loss or unavailability of this information for **less than one day** may cause (very) significant damage.

Integrity

Integrity is understood to mean: ensuring the accuracy and completeness of information and processing; it is a quality aspect that prevents information from being modified or destroyed either deliberately or inadvertently.

Elements of integrity, for example, include the making of changes by authorised persons, validity checks and the registration of changes, for example, by means of an audit trail or via a Change Acceptance Board (CAB).

In terms of integrity, the following classes are distinguished:

Class	Description
Low	The business process allows for a number of integrity failures. Changes in information or not harmful or are harmful to a very limited extent.
Medium	The business process allows for very few integrity failures. Inaccuracies can cause serious (in)direct damage.
High	The business process does not allow for integrity failures. Incorrect information can cause (very) significant damage.

Confidentiality

Confidentiality is understood to mean: ensuring that information is only available to those persons who are authorised to access that information.

Aspects that determine confidentiality include the encryption of information and user authentication for accessing the data.

The following classes are used with regard to confidentiality.

Class	Description
Public	All information that is generally accessible to everyone. A select group is allowed to make changes to this data. Disclosure does not cause any damage.
Internal (Low)	Information that may or should be accessible to persons affiliated with the AUAS. A select group is allowed to make changes to this data. Breach of confidentiality may cause some (in)direct damage.
Confidential (Medium)	Information that should only be accessible to a limited group of users. A select group is allowed to make changes to this data. Breach of confidentiality can cause serious (in)direct damage.
Confidential (High)	Highly confidential information, accessible only to specifically named individuals, where inadvertent disclosure outside this group may cause significant (in)direct damage.

The standard classification for personal data is as follows: Normal personal data is classified as Confidential, whereas Special personal data is classified as Confidential. The context of the situation, the use and the nature of personal data must always be taken into account, as these aspects may lead to the data being classified as higher than the standard classification dictates.

Characteristics of Availability, Integrity and Confidentiality

For further illustration, Bijlage A shows the characteristics and threats to Availability, Integrity and Confidentiality.

Level of protection

In order to apply proportionality between the value of the information and the costs of measures to be taken, security measures are divided into 3 levels of protection.

The following classes are used for the level of protection.

Class	Description
Low	This level contains the minimum requirements for all information facilities. The package of Standard Security Measures is also referred to as the 'security baseline'.
Medium	This level contains additional requirements in respect of the 'security baseline' for information facilities. The package of security measures entails additional requirements and additional costs.
High	This level contains additional requirements to the Standard and Sensitive levels. These may be standardised prescribed measures or they may be customised.

The table below shows the relationship between the level of protection and the classifications of the quality aspects of Availability, Integrity and Confidentiality.

Level of protection	Availability	Integrity	Confidentiality
Low	Low	Low	Low, Public
Medium	Medium	Medium	Medium
High	High	High	High

The classifications Low, Medium and High correspond to the level of protection. In addition, with regard to Confidentiality, the protection level Low applies to the classification Public.

The level of protection is determined separately for each of the quality aspects of Availability, Integrity and Confidentiality. This is to prevent a high level of protection for one quality aspect leading to expensive measures for another quality aspect with a Low level of protection.

8.2 Procedure

The process of classification will take place through interaction between the owner of the information and the CISO. The owner may also appoint a delegated owner and the CISO may also delegate a(n) (F)ISO or data steward.

The owner will share their assessment of the importance and business impact with the CISO, after which they will jointly draw conclusions and select appropriate measures. In many cases, this classification obviates a time-consuming and abstract risk assessment.

The three main phases of the classification are as follows:

1. Identification. Information classification starts with identifying what information is involved, what business process(es), information system and what laws and regulations may require its use, distribution and storage.
2. Impact assessment and level determination. Following identification, the classification of the information elements for the aspects of availability, integrity and confidentiality is determined; how big is the impact of breaches of these AIC aspects. These assessments lead to the determination of the (adequate) level of protection. Based on the protection level, the necessary associated measures are selected from the ‘Basic set of operational measures concerning information security’ [BOM].
3. Assessment of measures. This phase assesses whether the measures identified above are sufficient, whether they have already been implemented, or whether additional actions are required. If a classification of High has been determined or if there are standard measures that cannot or will not be taken, a separate risk assessment is required. All considerations and conclusions come together in the final recommendation.

8.3 Results

The result of the classification methodology is the classification and the measures to be taken for adequate protection of the information or the information system. This is recorded in the ‘IB&P risk assessment’ [IB&P] document.

The document is archived by the CISO, for the purpose of reproducibility, audits or to allow comparisons to be made for future reclassifications.

Bijlage A Characteristics of Availability, Integrity and Confidentiality

By way of illustration, the table below shows the characteristics of and threats to Availability, Integrity and Confidentiality.

Aspect	Characteristic	Threat	Example of Threat
Availability	Timeliness	Delay	Infrastructure overload
	Continuity	Downtime	Infrastructure malfunction
Integrity	Accuracy	Changes	Unauthorised modification of data; typing error
	Completeness	Removal	Unauthorised deletion of data
		Addition	Unauthorised addition of data
	Validity	Obsolescence	Not keeping data up to date
	Authenticity	Falsification	Fraudulent transaction
	Irrefutability	Denial	Denial of having sent a specific message
Confidentiality	Exclusivity	Disclosure	Network surveillance; unauthorised reading of documents; hacking systems or persons; loss and theft of laptop; data leaks.
		Abuse	Personal use to a large extent