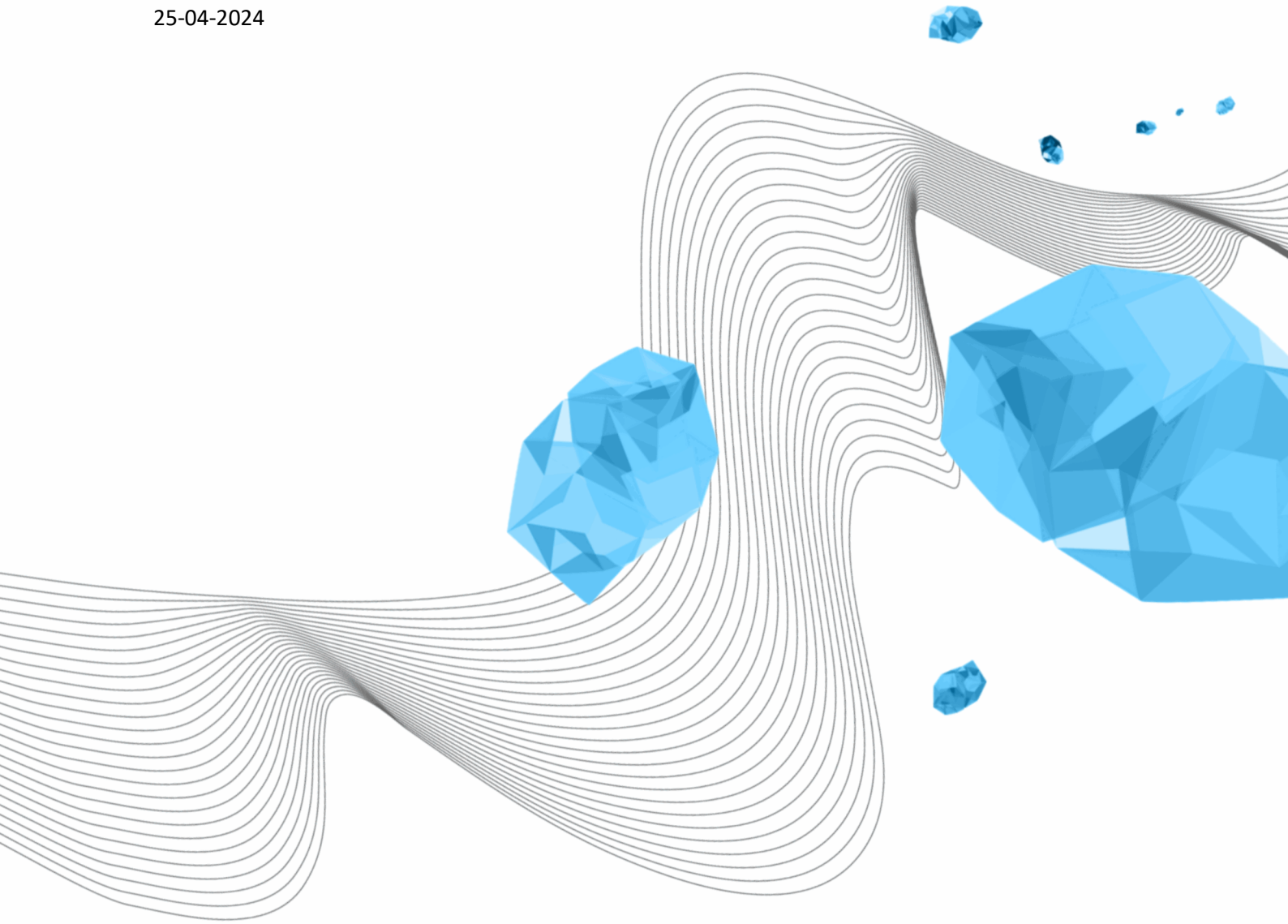
Status: Final
Date of adoption by LISA-MT: 29-04-2024
Revised: 25-04-2024
Author: Henk Swaters

CLASSIFICATION GUIDELINE INFORMATION AND INFORMATION SYSTEMS UNIVERSITY OF TWENTE

H.W.Swaters (LISA)

Version 2.1

25-04-2024



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
CLASSIFICATION GUIDELINE INFORMATION AND INFORMATION SYSTEMS UNIVERSITY OF TWENTE

ATTRIBUTE
LISA-397

VERSION (STATUS)
2.1

DATE
25-04-2024

AUTHOR(S)
H.W.Swaters (LISA)

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
2.0	24-4-2023	H.W.Swaters (translated by P.G.M. Peters)	Translated from the Dutch version
2.1	25-04-2023	H.W.Swaters (translated by P.G.M. Peters)	Updated version to be in line with the Dutch version numbering

DISTRIBUTION LIST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
2.0	24-04-2024	P. Peters	Henk Swaters
2.1	25-04-2024	P.Peters	MT-LISA

REFERENCE

VERSION	DATE	AUTHOR(S)	TITLE
2.0	23-06-2023	Henk Swaters	Classificatierichtlijn informatie en informatiesystemen Universiteit Twente

TABLE OF CONTENTS

1 INTRODUCTION

This document is a translation from the Dutch “Classificatierichtlijn informatie en informatiesystemen Universiteit Twente” version 2.0 from 23 June 2023.

This guideline elaborates on the Information and Information Systems classification described in the University of Twente Information Security Policy. This guideline is written to be used during the classification process without consulting the University of Twente's Information Security Policy.

1.1 GENERAL GUIDELINES

The University of Twente works with information and automated information systems. Attention to the security of information is necessary. This involves the right level of protection that matches the risks to which the information is exposed. Classification of information provides an estimate of the sensitivity and importance of the information and the associated degree of security. Classification, therefore, contributes to determining the correct degree of information protection.

As described in the University of Twente Information Security Policy, the classification must be determined by or on behalf of the owner of the information system in question. System owners (directors of services) have been designated for the UT's institutional systems, fulfilling the owner's role.

1.2 SCOPE

The classification system at the University of Twente relates to information (data) and the systems in which this information is stored (information systems).

Classification concerns all information (systems), both central and decentralised, to which the information security policy of the University of Twente applies.

1.3 OBJECTIVE OF CLASSIFICATION

Dealing with information is vital for the proper functioning of the University of Twente. Business operations, students, and employees must be able to trust that information is accessible when it is needed, correct and complete, and only available to authorised persons.

Not all information is confidential. So, protecting non-confidential information as strictly as highly confidential information could be more user-friendly. Proportionality is also desirable for efficient use of the available financial resources. A distinction should be made in protection. Classification is the tool for this.

2 PRINCIPLES AND FRAMEWORK

2.1 PRINCIPLES

At the University of Twente, the following principles apply to the classification of information and information systems:

1. The baseline information security is applied everywhere. These are the minimum prescribed security measures;
2. Where the risk analysis shows that additional measures are necessary, these must be taken;
3. The entire information security policy and measures are periodically subject to an audit;
4. Based on the audit results, new annual plans for information security are drawn up;

5. The classification is carried out under the responsibility of the System Owner of the information system.

2.2 FRAMEWORKS RELATING TO RELIABILITY

Below is a brief discussion of the frameworks that play a role in promoting the reliability of information. This concerns the concepts of Confidentiality, Integrity and Availability (CIA).

2.2.1 CONFIDENTIALITY

At the University of Twente, confidentiality means ensuring that information is only accessible to those authorised.

Elements of confidentiality include information encryption and user authentication as soon as they want to access the data.

2.2.2 INTEGRITY

At the University of Twente, integrity means guaranteeing the correctness and completeness of information and processing.

Elements of integrity include making changes by authorised persons, validity checks and registering changes.

2.2.3 AVAILABILITY

At the University of Twente, availability means ensuring authorised users have timely access to information and related facilities at the correct times.

Elements that determine availability include a reliable power supply, adequate fire protection, a current continuity plan, reliable backups and the absence of so-called 'single points of failure'. Other essential aspects are sufficient access options for the intended number of simultaneous users and protection against so-called 'denial of service' attacks.

2.3 CLASSIFICATION FOR INFORMATION

The class division below is used at the University of Twente for each of the CIA frameworks:

2.3.1 SECURITY CLASS 'STANDARD'

At the University of Twente, the classification standard means that the relevant system for the appropriate framework(s) must meet the minimum requirements imposed on all ICT facilities. The package of standard security measures is also called “baseline security”. The set of measures must be taken everywhere at the University of Twente, even if the classification does not give rise to additional measures.

If a system receives the standard classification, all standard security measures for the BIV aspects relevant to this system must be implemented.

2.3.2 SECURITY CLASS 'SENSITIVE'

The sensitive classification means that a breach of information's availability, integrity or confidentiality disrupts one of the primary processes but not of a very serious or irreversible nature. Possible adverse effects on the image of the University of Twente may also be a reason to assign a sensitive classification.

For systems with a sensitive classification on one or more of the CIA frameworks, an additional package of security measures will be prescribed compared to the “baseline security”. The sensitive classification, therefore, entails additional obligations and, thus, additional costs. The measures will usually still have a general, standardised character, whereby the costs can be expressed as extra costs in the service agreement.

2.3.3 SECURITY CLASS 'CRITICAL'

The critical classification is reserved for those systems where damage to availability, integrity and confidentiality causes a severe or irreversible disruption of one of the primary processes, seriously damages the image of the University of Twente or constitutes a violation of the law.

For systems with a critical classification on one or more of the BIV frameworks, additional measures must be taken on top of the measures for systems with a sensitive classification. These can again be standardised measures, but some customisation can also occur.

3 THE CLASSIFICATION PROCESS

The owner of the Information and the Information System is responsible for the implementation and result of the classification. The classification of information depends on the data in the information system and is supported by several questionnaires, with which the business impact is determined:

- General questions
- Questions about Confidentiality
- Questions about Integrity
- Questions about Availability

The business impact is assessed on a 5-point scale:

1. Negligible
2. Minor damage
3. Major damage
4. Serious damage
5. Threatens the survival of the institution

A translation can be made from the business impact assessments to the 3-point scale used for the CIA classification.

For the classification according to the insights of Confidentiality and Integrity, this translation can be as follows:

Business Impact	C or I classification
1 + 2	Standard
3	Sensitive
4 + 5	Critical

This division cannot be made directly for **availability**, but the resulting business impact assessment generally provides sufficient starting points to classify a critical, sensitive, and standard classification.

Which security level is suitable for a particular information system depends on the classification of the information that the system processes. The classification must be determined by or on behalf of the System Owner of the relevant information system.

In carrying out the classification process, the System Owner is supported by the Information Security Officer ISO (LISA), functional manager, application manager (LISA) and, if necessary, technical manager (LISA).

The questionnaires to be used can be found in Appendix A. For reasons of reproducibility, for example, if audit parties request background data and to enable comparison for future reclassification, the System Owner is advised to archive the completed questionnaires for future reference.

4 MEASURES

The classification result is determined per the CIA aspect at the University of Twente. The basis for this is the completed questionnaires. Based on the Business Impact, a Standard, Sensitive or Critical classification can be determined for all three aspects of Confidentiality, Integrity and Availability. If the highest security class is scored once in the questionnaires for C, I and A, this usually determines the class for the entire security aspect. This means that all measures belonging to that class of that aspect must be implemented.

The recommended measures will be periodically adjusted based on audit results, technical developments and new insights.

The Standard measures are the minimum (baseline) we always take. If aspect scores are sensitive, the sensitive measures are additional to the Standard measures. With the score Critical, the measures for Critical are additional to the measures for Standard + Sensitive.

4.1 ELABORATION OF MEASURES

To avoid repeating the exercise for each information asset to determine which measures must be taken, a matrix has been defined in which each classification is automatically linked to a set of minimum measures.

These measures are defined in broad terms and leave room for detailed interpretation unless there is a standard solution within LISA. Some of the measures described here are already operational. Some, however, still need to. Classifying the most critical institutional systems will determine the priority of implementing measures.

Although many measures are technical, it should be remembered that how users handle information is at least as necessary, if not more important, than the technical measures we can take. No technical measure can combat the irresponsible behaviour of users.

Cl.	Confidentiality	Integrity	Availability
Critical	• Secure printing environment? • Information may not leave the University of Twente buildings in printed form without the express permission of the System Owner • No copy of the production data may be used for testing purposes	• Synchronisation: real-time • Correction of errors: immediately after discovery • Authorisation: on mutation • Training all users • Periodic check of process/data • Use of digital signature in communication	• Redundancy: Fail-over • Backup: daily incremental, weekly full • Capacity planning through automated trend watching (daily control) • Breakdown service: 7x24

Cl.	Confidentiality	Integrity	Availability
Sensitive	• Authorisation by role • Not accessible via the public network. (VPN) • Information is logically not placed in the DMZ • Audit trail • Controlled disposal (both paper and digital) • Clear desk • Data will be distributed only with permission from the system owner.	• Synchronisation: within one business day • Correction of errors: within one business day • Authorisation: roll-based • Audit trail by mutation/user/role • Separation of duties • Training (core) users • Version management for documents, including time stamping	• Emergency power supply • Redundancy: Cold standby • Ransomware-proof backup: daily incremental, monthly full • Continuity plan/emergency plan in place • Capacity planning through automated trend watching (weekly check) • Support: opening of the University • Maintenance: outside office hours
Standard	• Encryption of data transport • Encryption of data storage • Authentication via personal username/password and 2-factor authentication • Strong password policy according to UT password policy • Passwords are sent via a secure encrypted connection • Anonymous data is used for testing purposes. If this is impossible, the same confidentiality regime applies as is the case with the production data. • For personal data, the purpose description, basis for processing, and, if applicable, the privacy test (DPIA) have been recorded. • LISA patch policy • Security monitoring by LISA	• Input Validation (server side) • Use of server certificate / SSL[1] • Preventing shadow files • Correction of errors: within agreed time • Authorisation: by group • Authentication via personal username/password and 2-factor authentication	• Data source is central • Redundancy: Spares • Backup: monthly emergencies • Capacity planning through automated trend watching (monthly check) • Support: opening of the service desk • Maintenance: In consultation with the System Owner. • LISA's patch policy always applies.

The explanation of the measures can be found in Appendix B.

5 IMPLEMENTATION

For new systems, the classification is carried out on behalf of the System Owner at the start of the project and discussed with the (C)ISO.

If changes affect the classification, the classification will be carried out again on behalf of the System Owner and discussed with the (C)ISO.

At the end of the project, the System Owner will test whether the information system complies with the measures in the classification. This can be carried out by LISA security management or an internal/external auditor.

The System Owner records the CIA classification results and shares them with the LISA IT Auditor to give a central overview of classifications.

Data classification is recorded in the LISA digital architecture wiki.

[1] https://www.utwente.nl/en/cyber-safety/protecting/protectingdata/FAQ-certificates/#security-information

6 REVIEW OF THIS CODE OF CONDUCT

This code of conduct is reviewed at least every three years. The following review will take place in mid-2026. There may be grounds for a mid-term review of this code of conduct. If this evaluation gives rise to it, the code of conduct will be amended sooner.

The CISO of the University of Twente is responsible for this code of conduct.

MT-LISA establishes this policy.

APPENDIX A: QUESTIONNAIRE

This appendix can be used as a fill-in document and as a basis for determining the classifications. Fill in the details below.

Document owner	
Function	
Department	
Phone number	
Enter last date	

GENERAL

1. Common name and a short description of the ICT facility.
2. For what functional purpose(s) is the ICT facility used?
   Consider main functions, such as administration, education, public information, etc. And user target groups.
3. What data is recorded in the ICT facility?
   Consider structure (texts, tables, images) and content (measurement results, personal details, locations, finances).
4. Is historical data recorded in or from the ICT facility or periodically written to other media?
   What is meant here is an internal or external archiving function and the regularity with which this happens, not the regular backup function.
5. How long is data kept online (after it has been processed commercially)?
   Consider diplomas issued, promotions, pension details, etc. Specify the terms, for example, after a year-end closing, graduation ceremony, or retirement.
6. Does the transport of authentication data occur to and from the ICT facility?
   Are there client/server connections or web interfaces? With which communication protocols?
7. How many people in which positions have the authority to change the ICT provision?
   Make a distinction here: authorisation of users, changes to system tables, entry of transactions, etc.
8. How many people in which positions have the authority to consult the ICT provision?
   Make a distinction here: general consultation function or personal data of the user himself, etc.
9. Does the ICT facility function as a source system for other systems, i.e. are data (files) provided to other systems?
   Specify the name and the System Owner for each receiving system.
10. Is this ICT facility the only one of its kind at the University of Twente?
    Please state any alternatives here (package, system, network component, etc.)
11. What types of workplaces are available for consultation or data modification?
    State the options for office, home/internet and mobile here.
12. Who is this system important for?
    This includes Organization as a whole, Process Owner, Users/process employees, and Registered Persons (customers, students, staff, suppliers, etc.)

CONFIDENTIALITY

Knowing the business consequences of unplanned or unauthorised disclosure or disclosure of that information is essential to determine whether and how confidential information is. A particular category of confidential data is personal data. We must comply with the General Data Protection Regulation (GDPR) when processing this. This allows a lot but does impose conditions on the processing and especially on the care taken in handling that data:

1. Are data stored or processed in the information asset that can be traced back to natural persons?
2. Does the information asset contain information that, combined with information from other systems, can be traced back to natural persons?
3. Does the information asset contain competitively sensitive data (e.g. rate structure, contracts)?
4. Does the information asset contain embargoed information?
5. Does the information tool contain information that may only be available to a specific target group? (also consider licensing restrictions)
6. Does the information asset contain data that could be used to commit fraud? (e.g. identity fraud, credit card numbers, password files).

Business impact scale:

1. Negligible
2. Minor damage
3. Major damage
4. Serious damage
5. Threatens the survival of the institution

Business Consequences	Business Impact				
	1	2	3	4	5
Competitive disadvantage How harmful is it if the information ends up with the competitor?					
Immediate loss of turnover Do we lose business/revenue if information is in the wrong hands?					
Public trust How significant is the damage to our image if this information becomes public, and how significant are the negative consequences for our customer's trust in us?					
Liability Can disclosure lead to liability based on legal or contractual obligations?					
Employee morale Does disclosure have adverse effects on employee morale or motivation?					
Fraud What impact do fraudulent actions have due to this data becoming known?					
Total score In summary, given the above scores (and possibly other consequences), what is the most significant damage that can be caused by unintentional or unauthorised access to this information? (this should generally be at least equal to the most extensive damage on an individual basis)					

INTEGRITY

In the context of integrity, it is essential to assess the possible consequences of errors in data. This applies to both intentional errors (or fraud) and unintentional errors.

While confidentiality concerns whether someone else can see the data, integrity is whether the other person can mutate the data. Key concepts are accuracy and completeness:

1. Does the data in the information resource form the basis for management decisions?
2. Which retention periods apply? (archive law, WBP, tax legislation, etc.)
3. Are there systematic checks for accuracy and completeness?
4. From what type of workplaces should data be available? (anytime and anywhere, at home, classrooms, staff workplace)
5. Can a user gain an unlawful advantage by deliberately changing a piece of data? (to commit fraud)
6. Maximum permitted data loss after failure?

Business impact scale:

1. Negligible
2. Minor damage
3. Major damage
4. Serious damage
5. Threatens the survival of the institution

Business Consequences	Business Impact				
	1	2	3	4	5
Management decisions How harmful is it if incorrect management decisions are made based on this information?					
Immediate loss of turnover Do we lose business/revenue if the information is changed without authorisation?					
Public trust How great is the damage to the image if incorrect information is used?					
Liability Can data inaccuracy lead to any form of liability?					
Employee morale Does disclosure have adverse effects on employee morale or motivation?					
Fraud What impact do fraudulent actions have?					
Total score Given the above scores (and possibly other consequences), what is the most significant damage that errors or unauthorised changes can cause? (this should typically be at least equal to the most extensive damage on an individual basis)					

AVAILABILITY

In the context of availability, it is good to look at the extent of the damage caused by a specific outage duration:

1. Which group of users is affected by a failure of the information asset? And how big is that group? What is the estimated number of concurrent users in the information asset?
2. What should be the opening hours for the information asset? What availability percentage is then desirable?
3. What frequency of system failure is still considered acceptable? (per month/quarter/year)
4. Has a Service Level Agreement (SLA) been agreed upon with LISA?
5. Is there a continuity plan for the information asset?

6. Are there critical failure moments? (e.g. payroll administration at the end of the month, reference date reports)
7. Maximum allowed downtime?

Business impact scale:

1. Negligible
2. Minor damage
3. Major damage
4. Serious damage
5. Threatens the survival of the institution

Business Consequences	**Business Impact**				
With an outage duration of	hour	day	2-3 days	week	month
Management decisions How harmful is it if wrong management decisions are made based on the unavailability of information?					
Immediate loss of turnover Do we lose business/revenue if information is not available?					
Public trust Is trust damaged, or is image damaged if an information asset is unavailable?					
Extra cost Do additional costs have to be incurred if the information asset is unavailable?					
Liability Can the unavailability of an application lead to any form of liability?					
Recovery What does it cost to clear the backlog of work after a restart?					
Employee morale Does it hurt user morale or motivation if the application is unavailable?					
Fraud Can the unavailability of an information asset lead to fraudulent actions?					
Total score In summary, what is the most severe damage that can occur in the event of failure at the most critical moment?					

BIJLAGE B: TOELICHTING OP DE MAATREGELEN

EXPLANATION OF CONFIDENTIALITY MEASURES

Several measures based on the principle of protecting integrity also apply to confidentiality. This mainly concerns measures related to authentication and authorisation. Measures in this area ensure that only authorised persons can make changes (integrity) and see specific information (confidentiality). These measures, therefore, appear in both columns in the matrix.

Authentication: This is about verifying someone's identity, so the requirements here relate to how someone can prove they are who they are. Authentication can take place based on something that one knows (e.g. password), has (e.g. token), or is (biometric characteristics, e.g. fingerprint). Two-factor authentication (or strong authentication) occurs when someone has to authenticate using a combination of two of these three.

The minimum requirement is a personal username with a password and a second factor. This makes it possible to trace actions to individual users.

Authorisation: Authorisation can be used to determine who can do what with which data. Group authorisation means that you get access to specific data because you belong to one particular group; you can, in principle, do anything with that data (e.g. access to parts of the P: drive). Authorisation by role means you get access to data because you fulfil a specific role within the organisation (purchaser, local planner, etc.). An authorisation for mutation is even more potent because it regulates access to the data and what you can do with it (reading, entering, changing, deleting, etc.). In practice, you often see combinations of roles with mutations (ERP is an example).

Firm password policy: In line with current guidelines.

Public networks: Confidential information may not be accessible via the public network (internet). This means that this information should not be logically placed in the DMZ. The DMZ (demilitarised zone) contains services that must be accessible from the Internet, such as a portal. If this information is to be accessible from home, VPN (virtual private network) facilities should be considered.

Encryption of data transport: Encryption of data transport is used to prevent eavesdropping. There are various tools available to monitor data traffic. These are tools used not only by hackers but also by network administrators to detect problems.

Encryption of storage: Nowadays, much information is carried on mobile devices (notebooks, PDAs, USB memory sticks, mobile phones, etc.). However, mobile devices are items susceptible to theft, and USB memory sticks can easily be forgotten. Confidential data stored on these devices must, therefore, be protected against reading by unauthorised persons. Also, critical information on Cloud services has to be protected.

Controlled disposal: Both digital media on which sensitive information is stored and the paper version must be disposed of in a controlled manner. The best way is to destroy hard drives and not reuse them. More than erasing alone is required (the literature states that only after seven overwrites does a hard drive no longer contain any recoverable information.) Printed versions of confidential information should be run through the paper shredder.

Clear desk policy: Confidential information should not be left lying on desks, even after working hours. After all, rooms are accessible to many people (cleaners, technical staff, service desk employees, colleagues, and emergency response staff.)

Complying with GDPR: The General Data Protection Regulation imposes several obligations about the careful manner in which personal data must be handled. The exemption decision linked to this law releases the University from the obligation to report to the AP for specific data processing operations. This does not alter the fact that the University must also comply with the law for these processing operations and must, therefore, have a purpose description, a basis for processing with, if applicable, a privacy test and approval from the Data Protection Officer. These must be recorded.

Distribution of data: The owner of confidential data must consent to the distribution of this data. This applies to both use in reports, for example, and the use of data by other systems.

Printing: If information needs to be printed, this must be done in a secure environment. Because printed information is, by definition, not encrypted, the System Owner must explicitly grant permission to use critical data outside the buildings of the University of Twente.

Test environment: Because a copy of the production database is often used for testing purposes, it is essential to maintain the same confidentiality regime for confidential information in the test environment as in the production environment. No copy of the production database may be used for critical confidential data for testing purposes. Whether a given is critical is sometimes also determined over time. Documents relating to merger discussions may be critically confidential during the discussions but may no longer be confidential after the merger has become a reality.

EXPLANATION OF INTEGRITY MEASURES

Synchronisation: Data integrity means that when data is used in different places in the organisation (often in other systems), it must be possible to assume that this data is also the same. In general, as much as possible, you should avoid shadow files (e.g., a telephone list in Excel while contact details are also on the portal). However, you cannot sometimes prevent data from being recorded and used in two places. Here, it is essential that one source system is designated, and agreements have therefore been made regarding the frequency at which the dependent systems receive an update of this data (= synchronisation). Real-time synchronisation is required for information assets classified as critical, meaning that source data changes must be implemented immediately in this dependent asset.

Correction of errors: Depending on the classification of the information asset, the speed at which corrections must be implemented following errors found will differ.

Authentication: This is about verifying someone's identity, so the requirements here relate to how someone can prove they are who they are. Authentication can take place based on something that one knows (e.g. password), has (e.g. token), or is (biometric characteristics, e.g. fingerprint). Two-factor authentication (or strong authentication) occurs when someone has to authenticate using a combination of two of these three.

The minimum requirement is a personal username with a password and a second factor. This makes it possible to trace actions to individual users. If you only have viewing rights from outside (website), then two-factor authentication is optional from the integrity point of view because you cannot change this data.

Authorisation: Authorisation can be used to determine who can do what with which data. Group authorisation means that you get access to specific data because you belong to one particular group; you can, in principle, do anything with that data (e.g. access to parts of the P: drive). Authorisation by role means you get access to data because you fulfil a specific role within the organisation (purchaser, local planner, etc.). An authorisation for mutation is even more potent because it regulates access to the data and what you can do with it (reading, entering, changing, deleting, etc.). In practice, you often see combinations of roles with mutations (ERP is an example).

Audit trail: This allows specific changes to be traced back to individual users. It provides capabilities to trace accidental errors and fraudulent actions back to a user.

Input validation: This allows you to prevent incorrect input to a certain extent at an early stage (think, for example, of a number that must be between 0 and 10 where it should not be possible to enter 11). The fact that this validation takes place on the server side and not on the client side (on the PC) is an important issue, especially with web applications. Inadequate input validation makes a web application vulnerable to “Cross-site scripting”. This is an attack technique in which a hacker sends small programs to the server via a web application's "input fields" and has them executed there.

Segregation of duties: This is an organisational measure that should be considered for specific processes. The susceptibility of processes to fraud can be reduced by ensuring that more than one person is needed to commit the fraud. (Consider the purchasing process; in this process, it is unwise to have the same person carry out the placing of an order, the receipt of goods and the payment of the invoice.)

Server certificates / TLS: Using server certificates lets users know whether the website they are accessing is correct and not a website that a hacker has recreated. In addition, information that the user exchanges with such a server is sent encrypted over the line. Server certificates can also be used to communicate between servers.

User training: This is an organisational measure. The integrity of company assets benefits from their correct use. Users must also be made aware of the security issues surrounding the processes of which they are part.

Version management of documents and timestamping: To prevent documents from appearing to be the same when they are not.

Periodic check of process/data: If integrity is critical, it will be necessary to regularly review whether the process and data still meet the integrity requirements and are carried out according to agreements.

Use of digital signature in communication: If the receiving party must be sure that a message comes from the sending party, he must be able to verify this via the digital signature (e.g. in the case of e-mail, this may be important). A digital signature works both ways; on the one hand, the recipient knows with certainty who sent the email, and on the other hand, the sender cannot deny that the email in question was sent by him (non-repudiation principle). Legally, a digital signature has the same status as a regular signature. These are, therefore, also valid for signing contracts, etc.

EXPLANATION OF AVAILABILITY MEASURES

Maintenance: Can be planned. This concerns the unavailability of a system at a pre-planned time. This time must always be determined in consultation with the System Owner. Information assets that score sensitive or critical in this regard must occur outside office hours.

Support: Refers to keeping the information asset available, including being able to answer questions from users about it. The service desk is open during office hours, and the university is open in the evenings and on Saturdays.

Breakdown service: Ensures a system remains available but does not answer user requests.

Backup: Spare copy. The frequency with which this is created partly determines the amount of lost data if, in the event of a disaster, data has to be restored (restored). An incremental backup only copies the changes compared to the last backup. The last full backup and all subsequent incremental backups must be restored during a restore. This determines the speed of the restoration.

Capacity planning: Capacity planning must provide timely insight into, for example, the filling of disks and crucial files (log files) and prevent performance problems. If disks or specific files become “full”, this can mean that a system is shutting down. Too many users on a system can cause slowness due to, for example, memory problems.

Redundancy: This is a double output of information assets to ensure you can continue working quickly in case of defects. Spares are spare parts such as a spare PC taken from the warehouse and still need to be installed to replace a defective workstation at a workplace. Cold standby means a second system is fully installed, but human action is still required to switch it on. Fail-over is a technique in which another system automatically takes over the function of the system in the event of a defect (without human intervention). The user (usually) does not notice this.

Source data centrally: Central means that you can also have backup facilities arranged centrally. With local storage, this is up to the individual user.

Continuity plans/contingency plans: A continuity plan mainly regulates the availability of business resources and business processes. It ensures that measures have been taken to resume processes quickly during a disaster. It also indicates priorities: which asset and process has priority? A disaster plan describes the actions that must taken in the case of a disaster. It usually contains an escalation plan and a contingency plan.

Emergency power supply: Ensures systems do not fail during a power failure. A power outage on systems not connected to an emergency power supply can affect the availability and integrity of the data on those systems. The speed at which these systems can be put back into the air is also adversely affected. After all, everything has to be checked before such a system can be rereleased for production.