UNIVERSITY OF GOTHENBURG

Division of Buildings and Services
Leif Bouvin
031 789 58 98

GOVERNING DOCUMENT
11-02-2015 Ref. no. V2013/414

Regulations for IT Security at the University of Gothenburg

Date of publication	June 2007 (rev. feb 2015)
Published	www.gu.se
Decision-maker	Vice-Chancellor
Date of decision	11-06-2007 (rev. new expressions 11-02-2015)
Person responsible for document	Leif Bouvin
Period of validity	Until further notice
Summary	Regulations for IT Security at the University of Gothenburg" sets out the regulations for use of the University's IT facilities, classification of information, procurement of systems and systems development, operation and maintenance, as well as protection of IT equipment and systems.

Division of Buildings and Services
Haraldsgatan 5, Box 100, SE 405 30 Göteborg
031 786 0000, 031 786 1142 (fax)
www.gu.se

Contents

Regulations for IT Security at the University of Gothenburg

1 Regulations for use of the University of Gothenburg's IT facilities

1.1 General

The University of Gothenburg's (GU's) IT facilities are owned by the University and are intended to be used in and for the University's function of providing education, research and associated administration, and also for cooperation with the local community. The facilities may not be utilised for purposes through which the University's name, prestige and good reputation may be damaged.

IT facilities refer to computers, mobile phones, tablets, software, software licences, communication networks and all other related equipment that is used in connection with communication and handling of information in digital form.

1.2 Regulations for use

1.2.1 Restrictions on the use of the University's IT facilities

The University's IT facilities may not be used to inappropriately or unethically distribute, store or convey information that

- contravenes applicable legislation, e.g. incitement to racial hatred, child pornography, illegal depiction of violent acts, slander, molestation, unauthorised access to computer systems or infringement of copyright
- without any connection with the user's role at GU, can be regarded as political, ideological or religious propaganda
- contravenes the provisions of the Personal Data Act regarding an individual's personal integrity
- is personally insulting or offensive
- is intended to market products or services unconnected to the University
- contravenes agreements made by GU regarding IT facilities
- or in any other way disrupts GU's IT operation

Private use of the University's IT facilities is only permitted to a limited extent.

1.2.2 Responsibilities and access rights

Before users are given access rights to GU's IT facilities, they must be informed of the current regulations for use and sign the "Agreement of responsible use of GU's IT facilities", or in some other way confirm that they are aware of the regulations, e.g. via a confirmation form in the Employee Portal.

User identity must always be traceable, which is why it is not permitted to use someone else's authorisation or exploit faulty configurations, program errors or in any other way manipulate the IT facilities.

The authorisation allocated is time-limited and is linked to studies, employment, and participation in a project or assignment. Users must themselves report circumstances that lead to cancellation of their access rights.

1.3 Regulations for internet and e-mail use

1.3.1 General

GUNET/SUNET are fast networks and a computer connected to them is therefore constantly exposed to attempts to gain unauthorised access (hacking). Information that is sent or made accessible via the internet can also be accessible to unauthorised persons. It is the responsibility of each user to protect GU's IT facilities against infringement and to protect information from access by unauthorised persons.

Consequently,

- computers and computer systems must always be protected by a securely constructed password, see point 1.5, or other technical authorisation and user identification
- computers owned/leased by GU must have antivirus programs licensed by GU and other security systems recommended by GU installed, and definitions must be updated
- other computers connected to GU's IT facilities must have equivalent security systems installed in order to attain sufficient protection, and definitions must be updated
- all attached documents/files must be tested for viruses before they are opened or downloaded onto the user's computer
- the user must never download programs and files onto a computer that is connected to GU's IT facilities without analysing the security risk
- all attempts to gain unauthorised access to computer systems must be reported to the University IT support or IT support for students
- confidential information requiring protection that is sent via e-mail, or that is made accessible via the internet, must be protected on the basis of the result of the completed information classification

If unsure regarding the application of the above regulations, contact University IT support or IT support for students.

1.3.2 Use of the internet

It is forbidden to use GU's IT facilities to unlawfully download material protected by copyright without permission from the rights holder.

GU's "Regulations for publication on the University of Gothenburg's websites" must be followed when publishing material online. If in doubt regarding publication of personal details, contact GU's personal data representative before publication.

An employee, that within the scope of his/her employment, uses a social media or cloud service must, before usage, consider the risks in relation to the information/material, that can be linked to the usage of the media or service. That means, for example, copyright, personal integrity and the content of the user

agreement or other contract. The risk assessment is conducted based on GU's regulations for information classification.

1.3.3 E-mail

All e-mails sent from addresses within GU represent the University. E-mails must contain correct information about the sender's name and address.

Before sending an e-mail, the address must be checked carefully to ensure that the message reaches the correct addressee.

1.3.4 E-mails handled by GU staff

E-mails are covered by the regulations for public documents. Registration of public documents, in the form of e-mails, must therefore take place according to the same regulations that apply to ordinary paper documents.

It is the responsibility of every employee to ensure that incoming e-mail is handled and that in their absence it is received and, if necessary, dealt with.

All e-mails received and sent to/from GU must go via GU's e-mail servers. Employees who need to handle e-mail for the University when not directly connected to GU's IT facilities must gain access to GU's own web services or other connection for this purpose set up by an approved technician. Automatically forwarding to external addresses of e-mail addressed to GU is not permitted. E-mail sent to GU must also be answered from a GU address.

1.4 Regulations for remote access to GU's IT facilities for staff

1.4.1 General

In order to maintain good security when using remote access, requirements are in place to ensure a high level of security throughout the communication process from user, equipment and program up to the IT service used.

To access some IT services users must themselves ascertain which regulations and instructions that the information owner and/or the system owner and IT-delivery manager have put in place for the IT services and IT systems in question.

1.4.2 Remote access from a private computer

In order to maintain a high level of security even when working from a private computer connected to one of GU's IT facilities, the computer must have at least an equivalent level of security as computers owned/leased by GU. The private computer equipment must have

- individual passwords, see point 1.5 below
- up-to-date antivirus software
- securely updated software
- connection approved by GU

For broadband connection, additional protection against unauthorised access must be in place through the installation of a firewall.

1.5 Regulations for passwords and logging in

The University's IT systems and each user must be protected by password and/or other technical authorisation and user identification.

In order to make protection derived from a password function effectively, the following criteria must be met.

- User identity, password and authorisation allocated must be personal.
- Passwords must be kept secret and not lent to anyone else.
- A password must consist of at least 8 characters in a mixture of upper and lower case letters, numbers and a special character. It must not be related to personal details such as name or date of birth, consist of simple words or similar and nor must it consist of keys that are in groups.
- The password must be changed every six months, or as soon as it becomes known to an outsider.
- The function to automatically lock the screen (power saving mode) after max. 10 minutes inactivity must always be switched on. To resume work at a work station the user must therefore unlock it by means of a password.
- The user must always log out from the computer when leaving the computer without the user's supervision.

1.6 Consequences and actions when regulations are breached

Any breach of these regulations may result in the user being completely or partially suspended from using the University's IT facilities. The decision is taken by the operational manager for the area of responsibility in question.

In serious cases, the IT-delivery owner may close down a mismanaged or misused IT facility with immediate effect.

Any breach of these regulations will be reported by the Head of Department/equivalent to

- the Vice-Chancellor in the case of students. The Vice-Chancellor will decide if the matter is to be referred to a disciplinary board. The disciplinary consequences entail a warning or temporary suspension from teaching and other activities at the University
- the staff disciplinary board in the case of employees. The consequences may be disciplinary responsibility or suspension.

Suspicion of crime can result in the police being notified.

2 Information classification

2.1 General

Information in its many forms is an important asset for the University of Gothenburg (GU). Classifying this information is a basic requirement for ensuring that the information is given essential and sufficient protection.

Developments within IT make it possible to handle (create, store, exchange and convey) information electronically to an increasing extent. Classifying the

information that is handled makes it easier to determine which electronic aids or services can be utilised.

Information at GU must be classified based on requirements regarding confidentiality, integrity (including traceability) and availability.

Processing of information that contains personal data must be reported to the University's personal data representative, who will provide instructions on how the information may be handled.

See further information in the University of Gothenburg's filing manual in the Employee Portal when determining whether or not a document is a public document.

The information owner is responsible for classifying his or her information, and for the classification being primarily based on the criteria of confidentiality, integrity (including traceability) and availability.

The table below gives examples of who counts as the information owner in different cases, unless otherwise agreed.

Category	Owner (unless otherwise specified)
Approved documents	The person who approved the document
Data in information systems	The system owner or the process owner
All other information	The issuer

2.2 Information classification

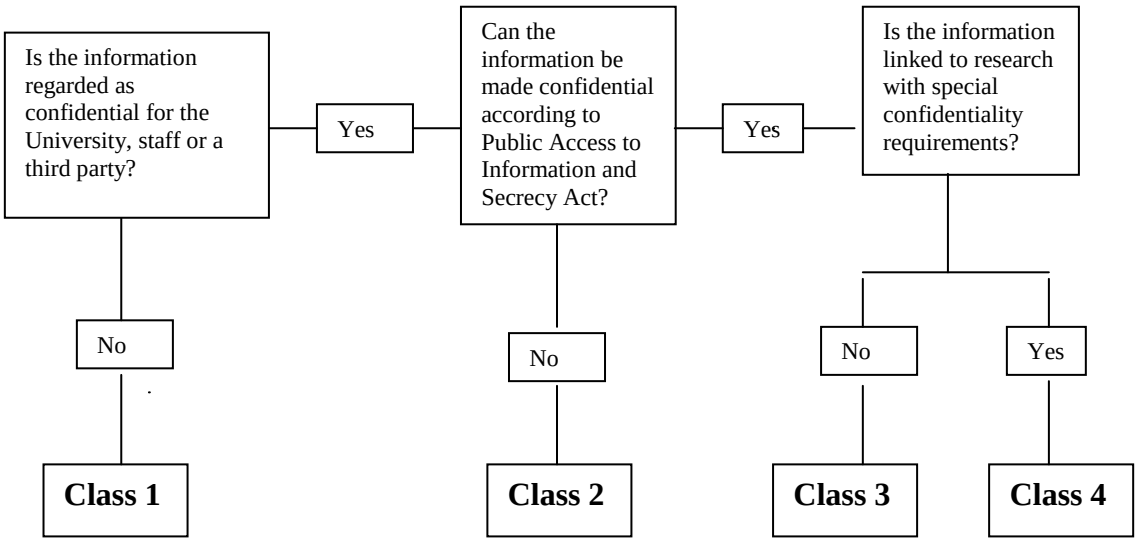
Information classification should ensure that the information is assigned an appropriate level of protection. To assist in this process, the criteria confidentiality, integrity and availability are used.

- **Confidentiality** refers to the information not being made available or revealed to unauthorised persons.
- **Integrity** (including traceability) refers to the information not being amended or corrupted unintentionally, or by unauthorised persons. **Traceability** refers to the creation and amendment of information being attributable to the person who created or amended it.
- **Availability** refers to the information being available to authorised users when needed.

The results from the three main classifications should constitute the overall requirement for protection of, and availability to the information or IT system in question.

2.2.1 Confidentiality

When classifying the information it must be assessed based on the confidentiality requirement, i.e. protection against the information being made available or revealed to unauthorised persons. The confidentiality requirement is classified in relation to the four information classifications detailed below, where information class 1 has the lowest requirement for confidentiality and class 4 the highest.



Class 1 confidentiality

The information may be stored on the work station's[1] local hard drive. The information may also be stored on portable media[2] without restrictions. The information may be transferred electronically without encryption.

The information may be sent via fax and ordinary mail, both internally and externally.

Class 2 confidentiality

In the first instance, the information must be stored on an independent server and not on the work station's local hard drive. The server must be located in an approved server room. The information may also be stored on portable media without restrictions. The information may be transferred electronically without encryption.

The information may be faxed, provided that a check is made of the recipient. A sealed envelope must be used when using internal mail. External mail handling may be used.

Class 3 confidentiality

The information must be stored on an independent server in a protected network. The server must be located in an approved server room.

In exceptional cases, the information may be stored on a work station, provided that the entire storage medium is encrypted and that the IT system does not distribute resources. The information may be stored on portable media, provided that the entire storage medium is encrypted and that it is locked away when not being used.[3] These media may not be left unattended or moved outside the University's premises unless being sent to another authorised recipient. All electronic transfer of the information must be encrypted.

[1] Work station refers to both stationary and laptop computers.
[2] For example, CD/DVD/USB memory stick/mobile phone/tablet/detachable hard drive/tape.
[3] Special procedures apply for backup copies.

The information may not be faxed and when being sent externally, registered mail and notice of delivery or alternatively a courier must be used. A double sealed envelope must be used when being sent by internal mail.

The information may not be stored in or synchronized with cloud services. [4]

When hard drives are changed, the hard drive replaced must be destroyed mechanically or alternatively overwritten according to standard DoD 5520-22.M with an overwriting program provided by GU, so that stored information cannot be reconstructed. Both the destruction certificate and signed overwriting memorandum must be filed.

Class 4 confidentiality

The information must be stored on an independent server in an isolated network and not on the work station's local hard drive. The server must be located in an approved server room, locked away separately.

In the event of a server not being available, the information must be stored on an encrypted separate hard drive that must be stored in a safe class SS 3492 when not in use. Laptop computers are to be locked away in an equivalent manner when not in use.

The information may be stored on other portable media, provided that the entire storage medium is encrypted and also that it is stored under lock and key in a safe class SS3492 when not in use. The portable media may not be left unattended or moved outside GU's premises unless being sent to another authorised recipient.

All electronic transfer of the information must be encrypted.

The information may not be faxed and when being sent externally, registered mail and notice of delivery or alternatively a courier must be used. The information may not be sent by internal mail.

The information may not be stored in or synchronized with cloud services.

When hard drives are changed, the hard drive replaced must be destroyed mechanically so that stored information cannot be reconstructed. The destruction certificate must be filed.

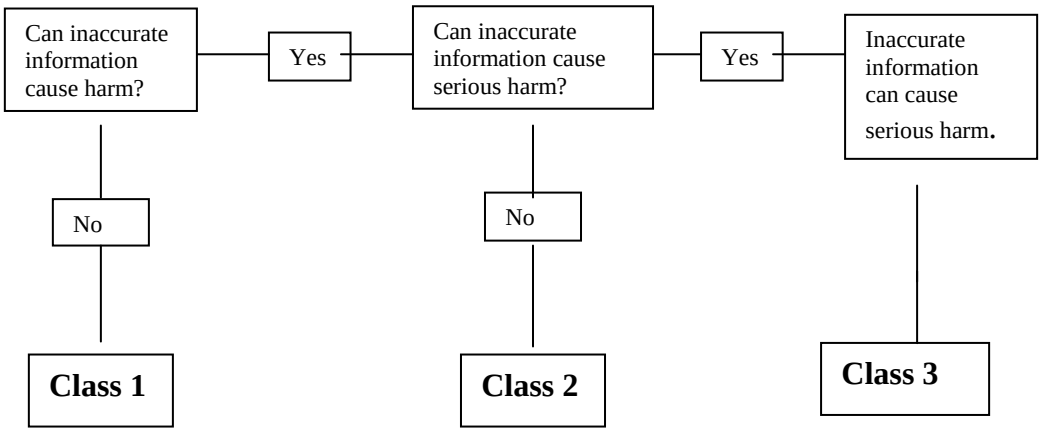
2.2.2 Integrity

When classifying the information it must be assessed based on the integrity requirement, i.e. protection against unintentional or intentional corruption.

In connection with classifying information in terms of integrity, the traceability requirement shall also be taken into consideration when assessing this information class.

The integrity requirement is classified in relation to the three information classes detailed below, where information class 1 has the lowest requirement for integrity and traceability, and class 3 the highest.

[4] Cloud services here refers to services that are based on resources shared by multiple users or organizations, and that programs and data are stored in a decentralized network of servers.



Class 1 integrity

No requirements are placed on verification of the integrity of the information or protection against corruption of the information.

Class 2 integrity

The information must be traceable and it must be possible to verify the integrity, for example by means of a signature.

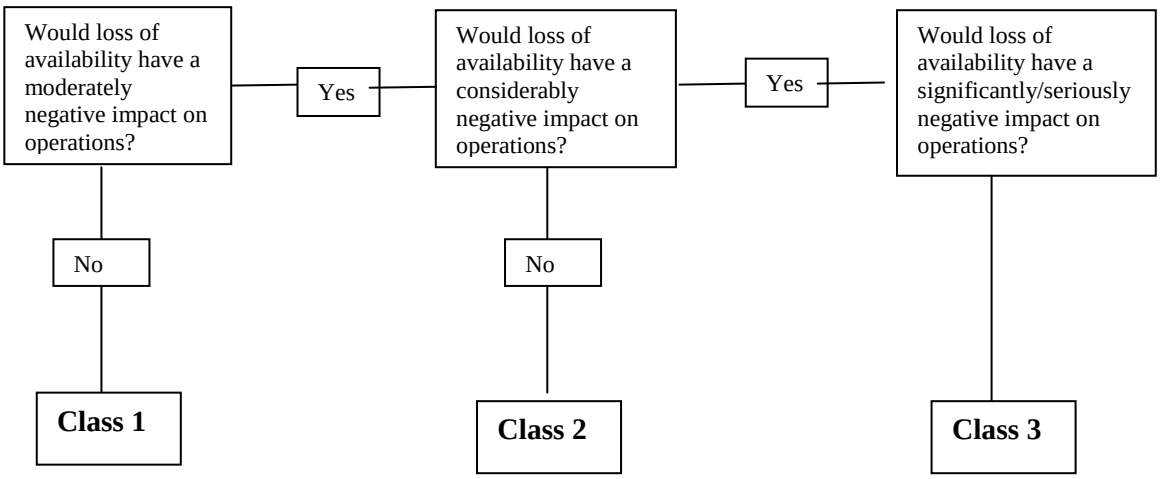
Class 3 integrity

Every input (transaction) or change of information must be traceable and it must be possible to verify the integrity of every input or change of information. The information must be provided with a high level of protection against unintentional or intentional changes and may only be accessed in a protected network with a customised authorisation control system.

The information may not be stored in or synchronized with cloud services with the exception of purchased services that comply with the requirements on verification of transactions.

2.2.3 Availability

When classifying the information it must be assessed based on the availability requirement, i.e. that the information is made available to authorised users when needed. The availability requirement is classified in relation to the three information classifications detailed below, where information class 1 has the lowest requirement for availability and class 3 the highest.



Class 1 availability

Moderate requirements are set in relation to availability of the information or the system.

Class 2 availability

Considerable requirements are set in relation to availability of the information or the system.

Class 3 availability

Significant requirements are set in relation to availability of the information or the system. Extended interruptions to availability are not acceptable.

Availability in accordance with the above applies primarily to availability in terms of time. Availability can be expressed in terms of both time and location. The location aspect, i.e. that the information should be available regardless of where the user is located, must take into account the increased risk of it not being possible to satisfy confidentiality and integrity requirements.

2.3 Summary

The result from the three different main classifications should constitute the overall requirement for protection of the information or IT system in question. The result constitutes the basis of how the owner of the information should handle the information and provides basic details of the system owner's requirement specification for an IT system.

3 Procurement of systems and system development

3.1 General

These regulations are in the first instance intended to control respectively the procurement and development processes for IT systems with several users, however where applicable they must also be taken into account when procuring and developing smaller systems for one or a small number of users.

3.2 Organisation and responsibility

3.2.1 Organisation

When procuring and developing smaller systems, the system owner and the IT-delivery manager jointly lead the procurement and development phases directly via the project manager.

When respectively procuring and developing larger IT systems with a large number of users and/or complex IT systems, a special project organisation must be created. The project organisation's steering group leads the procurement and development work up to the handover of the completed and documented IT system to the administrative organisation that is to be responsible for the future operation.

3.2.2 System owner

The system owner must be designated at an early stage in the respective processes of procurement and development. It should take place as early as the pilot study phase.

The system owner is responsible for ensuring that

- the information owner is identified for the information that the system will access
- the information owner's security requirements are implemented. The security requirements shall be stated with a focus on confidentiality, integrity, traceability and availability
- the planned system is designed and managed so that it fulfils the requirement for good information security
- the project organisation has access to the requisite IT security expertise
- in those cases where personal data is to be included in the planned IT system, this must be documented and reported to the University's personal data representative. The IT system must be designed so that it fulfils the requirements of the Personal Data Act
- an administrative organisation is created for the IT system's operation and maintenance with, in addition to a system administrator appointed by the system owner, a IT-delivery owner and a IT-delivery manager.

3.2.3 IT-delivery owner

The IT-delivery owner is responsible for ensuring that

- the information owner's and system owner's security requirements are fulfilled technically

- the technical security solutions comply with the standards set by the University of Gothenburg (GU)
- where appropriate, the system can be integrated with existing IT systems without impairing IT security
- the IT-delivery manager is appointed to the administrative organisation proposed by the system owner
- the IT system is entered into GU's system register in accordance with the "Regulations for Operation and Maintenance".

3.2.4 Project manager

The project manager is responsible for ensuring that

- the prescribed IT security activities are implemented and documented in the various phases of the project
- incidents and other events from a security point of view that have an impact on the project or the IT system's final security are reported to the system owner and IT-delivery owner.

3.3 Security management in the different phases of procurement and development

With the aim of achieving cost-effective and functional security solutions, the security aspects must be highlighted and the security requirements successively worked into the different phases of procurement and development.

3.3.1 The pilot study phase

An overall classification of the information that the IT system is to process must be included in the pilot study phase.

The information classification must provide answers to the following:

- the presence of personal data
- confidentiality requirements, e.g. the presence of information classified as confidential or other information of a sensitive nature
- requirement for the information's integrity and traceability
- requirement for availability.

3.3.2 The analysis phase

A security analysis must be carried out during the analysis phase. Threats and risks are to be analysed and documented in the security analysis, and proposals for measures formulated.

3.3.3 The procurement and/or design phase

System-specific security requirements and security measures that have been established are to be worked into the specification of requirements and the enquiry documentation, together with the general IT security requirements as set out in point 3.5 below, and the respective "Regulations for Operation and Maintenance".

Deviations from the established security requirements must be documented and reported to the information owner, system owner and IT-delivery manager for analysis and decisions.

Where appropriate, a report is to be submitted to GU's personal data representative.

3.3.4 Documentation

Supplier/designer provides user, training, operation and system documentation, as well as technical documentation. Documentation must be configured so that adjustments or updates can be inserted subsequently by parties other than the original designer of the IT system.

3.3.5 Test and handover

Test and control of the effect of security measures/solutions must be documented and approved by the system owner and IT-delivery owner before the IT system is put into production.

Upgrades and revisions to the IT system must be tested before they are put into production.

Tests must be carried out in special test environments. If a test in a special test environment is not possible, other suitable checks must be carried out in order to avoid operational disruptions or incorrect functioning when the IT system is put into production.

3.4 Training

It is the responsibility of the system owner to ensure that the requisite training of system managers and users is planned and implemented.

It is the responsibility of the IT-delivery owner to ensure that the requisite training of IT-delivery managers and system administrators is planned and implemented.

3.5 Fundamental security requirements for GU's IT systems

The fundamental security requirements below must, in both procurement and internal development of IT systems, be supplemented with the system-specific security requirements that emerge during the information classification and the security analysis during the pilot study phase or the analysis phase respectively.

3.5.1 Authorisation

Every user must have a unique individual user account/identity in order to ensure that only authorised users have access to the IT system. It must be possible to generate a list of the user identities used, with a link to the user's personal data (name and personal identity number).

It must be possible for the IT systems to utilise and be connected to an external module for authentication.

All authentications must be carried out in encrypted form.

3.5.2 Access and authentication control system

The IT systems must have a role-based access and authentication control system that can be adapted to the information owner's and the system owner's

requirements for security based on the organisation and security analysis carried out.

When necessary, it must be possible to generate access rights for availability of information for different levels within the organisation. Levels refer, for example, to laboratory, department, faculty or overall University level.

The IT system must be able to list current access rights by specifying

- the user's identity
- valid access rights linked to date of allocation and removal, and time limitation of authorisation.

3.5.3 Communication

Communication with the IT system must be protected based on the results of the completed information classification.

Any encryption must comply with a standard approved by GU.

3.5.4 Logging

All IT systems must have functions and procedures for logging security-related incidents in the system in order to ensure traceability, facilitate future investigations of operational disruptions and any irregularities and also for following up of the authorisation systems.

The incident logs consist of two main groups:

- revision logs (principally derived from the application log)
- operators' logs (principally derived from database and systems logs).

Logging must take place automatically and it must not be possible to corrupt or destroy them. Only in exceptional cases, when it is not possible to carry out automatic logging for technical reasons, is manual logging to be considered, on the basis of the protection value.

Revision logs with the function of registering deviations and other incidents relevant to security must be kept and stored for at least two years, or for the legally prescribed period.

Logs concerning financial transactions, for example in accounting and personnel administration systems, must be kept for 10 years.

The operators' logs are to be saved for at least six months, or for the legally prescribed period.

3.5.5 Special IT security requirements

Firewalls
Procurement and configuration of firewalls must comply with a standard stipulated by GU.

Virus protection
It is the responsibility of system owners and the IT-delivery owner to plan and verify that relevant antivirus software is installed for each IT system under their responsibility.

Certificate
In those cases where IT systems utilise certificate-dependent encryption, a certificate recommended by GU's IT unit must be used.

Wireless networks (radio LAN)
When new wireless networks are set up within GU, GUWLAN, the common format that has been developed for the University, must be used.

3.5.6 Assessment of suppliers

With the aim of guaranteeing the supplier's future obligations, an assessment of the supplier must be undertaken in consultation with GU's Procurement Unit.

With regard to the results of the completed information classification, as well as the risk and security analysis, suppliers, collaborative partners or other supplying organisations must be assessed on the basis of the same requirements as are set out in point 3.7 "Fundamental security requirements for IT operations through external suppliers".

3.5.7 Source code deposit

Deposit of source codes for GU's IT systems must be well documented and take place in a way that safeguards future operating, supplementing and maintenance of the IT systems. In addition, the following applies:

- When procuring IT systems, deposit of source codes must be regulated in an agreement.
- When IT systems are developed in-house, it is the IT-delivery owner's responsibility for ensuring that the source code is deposited/filed in a secure manner.
- Deposit/filing must meet "the National Archives' regulations and general advice on premises for archives" (RA-FS 2013:4).

3.5.8 Reliability

To maintain a high level of availability and to reduce the risk of losing information, GU's IT systems must be designed in order to provide a high level of reliability and be equipped with an administration module that is easy to operate. Support and maintenance must be guaranteed for the system's entire lifespan. This is documented in the system management plan.

3.6 Phasing out IT systems

A plan both for phasing out IT systems and principles for how essential data is to be saved must be developed as early as the planning stage.

3.7 Establishment of security requirements for IT that is operated through external suppliers

3.7.1 Security organisation

The supplier must have a security organisation in place with a responsible manager and a named contact person for security issues. The contact person for security issues should be specified in the agreement with the supplier.

The supplier must provide GU with an account of the security policy and guidelines regarding

- physical security
- IT security
- confidentiality

Any changes to the named policy and guidelines must be reported to the contact person appointed by GU. Following assessment, the whole of the policy and guidelines, or parts thereof, can be attached to the agreement if necessary.

3.7.2 IT security policy and guidelines

In general, the supplier must comply with GU's IT security policy and the regulations and guidelines linked to it.

On completion of an assignment

- the supplier must return classified and sensitive material
- electronically stored information must be deleted/destroyed in accordance with GU directives
- all system documentation must be returned to GU.

3.7.3 Confidentiality and vetting of personnel

Confidentiality

The following confidentiality clause must be included in the agreement regarding IT operated through an external supplier:

The supplier will undertake to comply with applicable security regulations determined by the University of Gothenburg from time to time, and guarantees that they will be observed by staff/consultants and subcontractors that are engaged.

In those cases where the supplier is given access to information protected in accordance with the Public Access to Information and Secrets Act (2009:400), the applicable regulations in the aforementioned act must be observed. The supplier must provide information to staff/consultants and subcontractors that are engaged regarding applicable confidentiality. Confidentiality also applies if the agreement otherwise ceases to apply.

The supplier may not surrender documents to third parties or in any other way reproduce information about the University of Gothenburg's activities that might be considered commercially or professionally confidential or that in general concerns the University of Gothenburg's internal circumstances, other than to the extent required to undertake the assignment.

Vetting of personnel

The supplier must give an account of the type and scope of security checks carried out before each member of staff is permitted to work on the assignment for GU.

The checks must comprise at least

- personal information
- information set out in reports, certificates and references.

A security assessment is made of the supplier's responses based on the results of the information classification and security analysis that has been carried out.

3.7.4 Handling of confidential information

In addition to that which is specified in GU's regulations and guidelines for "5. Protection of IT equipment and systems", the following regulations must be followed.

- Confidential and sensitive information must be handled and stored in a way that prevents unauthorised persons from gaining access to it. Such information must be stored in a computer media cabinet that, in addition to the environmental requirements, fulfils the requirements for security cabinets as set out in SS 3492.
- All electronic communication of confidential or sensitive information must be encrypted with respect to the results of the completed information classification.
- Documents and portable media must be transported in a locked briefcase by the supplier or GU's staff.
- Any forwarding by post must take place using an ESS letter, registered.

3.7.5 Handling of discarded memory media

Disposal of memory media must be carried out as set out in GU's regulations and guidelines for "5. Protection of IT equipment and systems".

3.8 Fundamental security requirements when using external IT consultants

The assignment as IT consultant means that suppliers and/or their subcontractors

- work on the University's premises and handle or can access confidential and sensitive information
- are allocated personal access rights for GU's IT facilities.

3.8.1 Security organisation

The supplier must have a security organisation in place with a responsible manager and a named contact person for security issues. The contact person for security issues should be specified in the agreement with the supplier.

Only staff named in the agreement may be used for the assignment. Changes of named persons must be approved in writing by GU.

Staff must be able to prove their identity by means of an identity document issued by the supplier.

3.8.2 Physical security

In the assignment contract

- the supplier must undertake to comply with the University's security guidelines regarding entry to the premises
- the supplier must undertake not to remove any confidential or sensitive documents, files, portable media, material or other information from the University's premises, and to comply with GU's regulations and guidelines for storage of this type of material and information.

3.8.3 IT security

The supplier must comply with GU's IT security policy and the regulations and guidelines linked to it.

Files or software may not be transferred to networks outside GU's networks without special permission.

3.8.4 Confidentiality and vetting of personnel

See point 3.7.3 above.

4 Operation and maintenance

4.1 System administration

4.1.1 System register

The University of Gothenburg's (GU's) common IT system and the IT systems of each faculty board must be registered at each organisational level by stating:

- system register
- information owner
- system owner
- system manager
- IT-delivery owner
- IT-delivery manager
- whether the system contains personal data.

4.1.2 Roles

In the everyday operation and maintenance of IT systems and infrastructures, system owners are to be supported by

- a system manager appointed for each system.

In the everyday operation and maintenance of IT systems and infrastructures, the IT-delivery owner is to be supported by

- a IT-delivery manager appointed for each IT system and infrastructure
- one or more system administrators.

4.1.3 Agreements of responsible use for IT staff

Before staff are given authorisation to work on operation and maintenance of GU's IT facilities they must be informed of the applicable rules and regulations for IT security at GU and sign the agreements of responsible use below, or in some other way confirm that they are aware of the regulations:

- Agreement of responsible use of the University of Gothenburg's IT facilities.
- Agreement of responsible use for employees with higher technical and administrative access to the University of Gothenburg's IT facilities.

4.1.4 Decisions and documentation of system changes

Decisions on system changes are made by the respective system owner, in consultation with the IT-delivery owner.

The system manager and IT-delivery manager are responsible for ensuring that both decisions on system changes and the implemented changes are documented and filed in a secure manner that permits

- follow-up of system changes that have been made
- any handover by both system management and technical management.

4.1.5 Testing prior to commissioning

All system changes must be tested in a special test environment before commissioning. If testing in a special test environment is not possible, other suitable checks must be carried out in order to avoid operational disruptions or incorrect functioning when the system change is put into production.

4.2 Authentication administration

4.2.1 Basis

A functional and secure administration of access rights is one of the most important basic features of GU's IT security work.

Users may only be allocated access rights to GU's IT facilities to the extent required for their work assignments or studies.

General authorisation

Before users are given access rights to use GU's IT facilities, they must be informed of the applicable regulations for use and sign the "Agreement of responsible use of GU's IT facilities", or in some other way confirm that they are aware of the regulations, e.g. via a confirmation form in the Employee Portal.

Access rights for IT systems with special authorisation rules

Guidelines for allocation of access rights for specific IT systems are regulated by the respective information owner/system owner.

4.2.2 Roles

Information owner

Based on information classification rules and completed security analyses, the respective information owner is responsible for drawing up rules for the allocation of access rights in consultation with the system administrator.

System owner
The system owner is responsible for ensuring that the information owner's rules for the allocation of access rights are complied with.

IT-delivery owner

It is the IT-delivery owner's responsibility to ensure that the information owner's and the system owner's security requirements for authentication control are fulfilled technically and that logs are backed up, saved and stored in a secure manner for the prescribed period.

Authorisation manager

Authorisation managers decide on allocation of access rights to the University's common and local systems, and are also responsible for following up access rights that have been allocated. Allocation and follow-up must comply with guidelines set by the information owner, system owner and IT-delivery owner.

Authorisation managers are heads of department, heads of division in Central Administration, university managers within the University Library, heads of faculty offices, national unit representatives or equivalent.

Authorisation administrator

Authorisation administrators are appointed by authorisation managers and are responsible for registration and deregistration of access rights, in accordance with the decisions of the authorisation manager. The administrator is also responsible for ensuring that decisions on allocation of access rights are filed according to the stipulated filing regulations.

4.2.3 Documentation and filing of authorisation decisions

Agreements of responsible use of GU's IT facilities and decisions for allocation of access rights for IT systems with special authorisation rules must be kept for two years after the authorisation has come to an end.

Decisions on allocation of access rights with regard to financial transactions in, for example, the accounting system and the personnel administration system must be kept for 10 years.

Documentation of decisions on allocation of access rights must

- be stored under lock and key to prevent access by unauthorised persons
- be stored as set out in applicable filing regulations to prevent unintentional destruction by fire, or similar.

4.2.4 Removal of access rights

It is the responsibility of the authorisation manager to ensure that users' authorisations are immediately removed when they leave their employment, finish their studies or equivalent at GU, and that the access rights are updated when job assignments or studies change.

The authorisation manager is responsible for ensuring that an annual review is carried out of the allocated access rights in relation to

- current user lists
- lists drawn up by the system owner of allocated access rights.

The allocation of access rights must be updated and edited on the basis of this review.

4.3 Security measures to reduce the consequences in the event of disruptions (continuity planning)

4.3.1 Backup copying

The purpose of backup copying is to guarantee availability to IT systems and stored information.

Backup copying must be carried out regularly.

Based on the information classification carried out and the frequency with which the information is changed, in consultation with the IT-delivery manager, the information owner/system owner must decide on and document

- which information is to be covered by backup copying
- time interval for backup copying
- which standards for backup copying are to be followed

- when and how the legibility of backup copies is to be checked and documented.

All IT systems must be backed up for security reasons on installation, as well as before and after major changes.

It must be possible to recreate IT systems and stored information on other hardware.

4.3.2 Protection of backup copies against fire and theft.

Backup copies are to be stored in a server room or a fireproof computer media cabinet located in a fire cell other than the one in which the original information is stored.

4.3.3 Handling of operational incidents

It is the IT-delivery owner's responsibility, together with the system owner, to ensure each system plan contains documented procedures for dealing with operational incidents for each IT system. The documentation should address the following points.

Risk analysis
Display conceivable scenarios and measures

Reporting procedures
Information on who should be informed at different stages.

Contacts

Supplier undertakings
Documentation on the agreements that apply for hardware guarantees, call-out time, support in the event of operational incidents etc.

Documentation and analysis
Operational incidents must be documented and analysed in order to acquire knowledge about what happened, to avoid new incidents in the future, and to reduce the time needed to take action in the event of similar incidents in the future.

4.3.4 Handling of security incidents

Unauthorised access (hacking)

In cases of hacking where persons have unlawfully acquired authorisation to IT systems, the Incident Response Team at GU must be contacted. The intrusion must be analysed so that relevant measures can be taken to prevent similar intrusions being repeated. When system administrators (equivalent) can establish that the IT system has been taken over by unauthorised persons, the system must be restored by reinstalling and re-inputting the backup copy taken before the intrusion. All users of the system affected must be provided with new passwords and if any users utilise several systems for which they use the same password then these must also be changed.

Viruses/worms

In case of unauthorised access caused by viruses/worms, the system must be rectified with the antivirus programs provided by GU. In those cases where the system administrator (equivalent) deems that this is not sufficient, the system must be reinstalled. The cause of the virus/worm attack must be analysed to enable appropriate measures to be taken to prevent recurrence.

Misuse

Discovery of internal hacking such as extension of individual access rights, manipulation of data, unauthorised viewing or accessing of digital information etc. must be reported to the head of department or equivalent, who will inform GU's security officer, who then follows the "Procedure in the event of misuse of the University of Gothenburg's IT facilities".

4.4 Logging and log analyses

4.4.1 Types of logs

All IT systems must have functions and procedures for logging security-related incidents in the system in order to ensure traceability, facilitate future investigations of operational disruptions and any irregularities and also for following up of the authorisation systems.

The incident logs consist of two main groups:

- revision logs (principally derived from the application log)
- operators' logs (principally derived from database and systems logs).

Logging must take place automatically and it must not be possible to corrupt or destroy them. Only in exceptional cases, when it is not possible to carry out automatic logging for technical reasons, is manual logging to be considered, on the basis of the protection value.

To enable logs to be used effectively to investigate security incidents and as evidence in any legal trial, the IT-delivery ownerechnical officer is responsible for ensuring

- that clocks between different systems are synchronised according to GU's time server
- that the logs are stored securely and have backup copies that are stored under lock and key in another fire cell (see point 4.3.3).

Revision logs with the function of registering deviations and other incidents relevant to security must be kept and stored for at least two years, or for the legally prescribed period.

Logs concerning financial transactions, for example in accounting and personnel administration systems, must be kept for 10 years.

The operators' logs are to be saved for at least six months, or for the legally prescribed period.

4.4.2 E-mail communication traffic log

For the purpose of being able to investigate from a security perspective whether e-mail has arrived at or been sent from GU, logs (traffic lists) of e-mail communication must be saved for two years. See also GU's filing manual.

4.4.3 Checking and monitoring log information

On the basis of the system owner's security requirements, logs must be regularly checked with respect to abnormal circumstances and security incidents. Withdrawal of log information must be based on the decision of the system owner

with regard to the individual system, the IT-delivery manager with regard to the individual IT network, GU's security officer or auditor.

Decisions on withdrawal of log information must be in writing and justified by

- preventive auditing or security follow-ups
- security-related incidents, or a suspicion of such.

It must be possible to export the logs to text format to enable analysis in external analysis tools.

4.5 Other specific security procedures

4.5.1 Firewalls

Procurement and configuration of firewalls must comply with a standard stipulated by GU.

4.5.2 Virus protection

All incoming and outgoing e-mails must be checked for viruses and all file servers must have virus protection approved by GU.

It is the responsibility of system owners to plan and verify that relevant antivirus software is installed for each IT system under their responsibility.

It is the responsibility of the IT-delivery owner to technically implement and verify that the virus protection is working.

4.5.3 Junk mail (spam)

Spam refers to mass mail-outs of unwanted, unsolicited e-mails, often with a commercial message and without the consent of the recipient.

As a public body, the University has to safeguard the opportunities the general public and the students have to communicate with the University via e-mail. GU recommends openness but must oppose spam, in so doing the University must use methods and take measures with the aim of reducing both outgoing and incoming spam.

This means that as a matter of routine, the University will reject e-mails that can in all certainty be considered to be spam.

The University will follow technical developments and take the technical measures that provide the optimum results to counteract spam.

Spam filters that are based solely on "blacklists" may not be used at the University.

Every e-mail that is not deemed to constitute spam will be dealt with so that it reaches its addressee.

4.5.4 Encryption

Based on the results of the completed information classification, the communication and storage of the information in the IT system must be encrypted.

All authentications must be carried out in encrypted form.

Encryption must comply with GU-approved standards.

4.5.5 Certificates

In those cases where IT systems utilise certificate-dependent encryption, a certificate recommended by GU's IT Department must be used.

4.5.6 Wireless networks (radio LAN)

When new wireless networks are set up within the University of Gothenburg, GUWLAN, the common format that has been developed for the University, must be used.

5 Protection of IT equipment and systems

5.1 General regulations regarding technical security requirements for design of rooms for main distribution frame and communication equipment, server rooms and computer rooms

With the aim of protecting the University of Gothenburg's (GU's) IT infrastructure, applications and stored data against unintentional damage due to fire and leaks of liquid, intentional damage and unlawful use respectively, the rooms for main distribution frames and communication equipment, server rooms and central computer rooms must be designed according to the technical security requirements stipulated by GU's security officer.

The regulations are to be perceived as minimum requirements and utilised for new buildings and conversions and also as targets for gradual increases in the IT security in existing premises. With respect to the nature of the activity, the result of risk analyses and the opportunities for the emergency services to intervene, it is primarily the fire protection requirements that might need to be enhanced.

5.2 Storage of backup copies

Backup copies are to be stored in a server room or a fireproof computer media cabinet located in a fire cell other than the one in which the copied information is stored.

The server room must comply with the technical security requirements stipulated by GU's security officer.

The computer media cabinet must be tested and approved for computer media as set out in Swedish standard SS-A 1047-1. If confidential information is stored in the cabinet it must also meet the requirements for security cabinets class SS3492.

5.3 Filing of information on IT media

Filing of information stored on IT media must be carried out in rooms or cabinets that comply with "the National Archives' regulations and general advice on premises for archives" (RA-FS 2013:4).

Detailed requirements are set out in GU's filing manual.

5.4 Protection of stationary and portable work stations and video projectors

5.4.1 Stationary work stations

Stationary work stations in more open environments, such as corridors, computer rooms, reception areas and in premises equipped with windows that can easily be accessed from the outside, must be securely locked. Computers are to be placed in anti-theft boxes approved by the security officer and screens are to be securely locked with wires, chains or other locking devices recommended by the security officer.

In very exposed environments, the work station should also be fitted with an alarm.

5.4.2 Laptop computers

Laptop computers must be fitted with equipment for temporary locking.

In regular workplaces it should be possible to securely lock laptop computers or alternatively lock them in a cabinet.

5.4.3 Video projectors and large flat screens

Stationary video projectors and large flat screens are to be mounted in a security casing or locking device recommended by the security officer and be equipped with an alarm linked to the property's burglar alarm.

Portable video projectors must be fitted with equipment to enable temporary secure locking and when used in exposed environments, an acoustic alarm should also be considered.

5.4.4 Anti-theft marking

All IT equipment such as stationary and portable work stations, including screens, video projectors, plasma screens in entrances and similar must be marked with an anti-theft label. See also GU's finance manual, chapter 7.

5.5 Taking care of IT media and equipment that is to leave the University

5.5.1 General

To prevent stored information such as personal data, research data, confidential information and similar becoming available to unauthorised persons, all discarded memory media must be deleted and overwritten or destroyed mechanically in a secure manner.

Memory media that contain confidential information must be both overwritten and destroyed mechanically.

In this context, memory media include all electronic equipment containing a memory function, such as fixed and detachable hard drives, handheld computers including mobile phones with handheld computer functionality, USB memory sticks, CDs, tapes, diskettes and other detachable memory units.

Printers with in-built memory functions must also be deleted and overwritten in a secure way before they leave the University.

5.5.2 Computers and detachable memory media that are to be sold or handed over to external ownership

In addition to the regulations in GU's finance manual chapter 7, when computers and detachable memory media are sold or otherwise handed over to external ownership, stored information must be deleted and overwritten in accordance with standard DoD 5520-22.M. The overwriting must be carried out with one of the overwriting programs approved by the IT Department.

Computers and detachable memory media that contained confidential information may not be sold or otherwise handed over to external ownership. After overwriting, these are to be mechanically destroyed, see 5.5.3 below.

The overwriting process is documented on form "Report of deregistration of fixed assets". The documentation must set out the date for the overwriting, who carried out the overwriting and which overwriting program was used.

5.5.3 Computers and detachable memory media that are scrapped

According to the statute (2000:208) on producer responsibility for electrical and electronic products, suppliers of electronic equipment have to take back discarded and scrapped IT equipment. For discarded and scrapped memory media to be returned to the supplier, the supplier must be able to display one of the processes approved by GU's security officer for secure/safe destruction.

Heads of department, heads of division in Central Administration, university managers within the University Library, heads of faculty offices, national unit representatives or equivalent are responsible for ensuring that discarded and scrapped memory media are taken charge of and destroyed in a secure process approved by GU's security officer, from GU's premises to mechanical destruction.

Tablet computer, Smartphones, mobile phones, USB memory sticks, CD, tapes and other devices that contain or have contained sensitive or confidential information must be destroyed mechanically or placed in a container approved by GU's security officer for secure destruction of paper. For memory media from commissioned research or equivalent with special secrecy requirements, GU's security officer must be contacted.

The destruction is documented on form "Report of deregistration of fixed assets". The documentation must specify the date and to whom the equipment was handed for destruction. A destruction certificate from the destruction firm or the supplier that took back the equipment must be filed by the respective IT-delivery manager.