CHALMERS

| | | | |
|---|---|---|---|
| **Decision by:**<br>Ida Rosengren | **Type of policy document:**<br>Regulation | **Registration number:**<br>C 2020–0420 | |
| **Date of decision:**<br>06/11/2020 | **Administrator:**<br>Anders Qvist, Information Security Coordinator | **Document structure:**<br>D1.3 | |
| **Document effective from:**<br>06/11/2020 | **Division/equivalent responsible for creating and/or revising the document:**<br>Management Support | **Document revised, date:** | **Version number:**<br>1.0 |
| **Document effective to:**<br>Until further notice | **The document supersedes earlier decision:**<br>Information security regulations (C 2018-0167) and<br>Research information regulations (C 2018-0168) | **Document reviewed without change, date:** | |

# Information security regulations

## Policy document at Chalmers

## Contents

# 1. Background and contents

These regulations are part of Chalmers' management system for information security. The regulations govern how operational information is handled in a secure manner while complying with Chalmers' regulations and applicable laws. The document is based on previous recommendations and established guidelines for the handling of operational information and research information.

The regulations contain:

- Rules regarding responsibility
- Classification and management of operational information
- General information security requirements
- Rules regarding procurement and purchasing
- Regulations for the use of Chalmers' IT resources
- Specific advice and tips regarding information security in relation to the following areas:
  - Incident investigation
  - The handling of personal data
  - Archiving and public access principles
  - Collaboration with external parties

## Recipients

Recipients of the regulations are both staff members and external parties who are active in or have a relationship with Chalmers and use Chalmers' IT resources and process Chalmers' operational information. Included in the classification *staff member* are researching and teaching staff, technical and administrative staff, and those in teaching positions and specialist positions. Managers have special responsibility for ensuring compliance with the regulations within their respective operations.

Examples of those classified as *external* include the following:

- External partners
- Research collaborations
- External consultants
- Other stakeholders

## Research

The regulations will indicate how the handling of research information may differ from the handling of other operational information. This is clarified using boxes with the heading "*The following applies for research*" that contain a more detailed risk description for this area.

## Key components and management

In the information security management at Chalmers, the key components *confidentiality*, *integrity* and *availability* are taken into account, where deficiencies in management of these put concerned parties at increased risk of unknown harm.

- Confidentiality means that information is protected from access by unauthorised individuals, objects and processes.
- Integrity means that information is correct, current and complete. Information may not be changed in an unauthorised manner.
- Availability means that information can be accessed by authorised individuals, objects and processes at the right time.

***The following applies for research:***
Improper handling of research information can make patenting and publication of research results impossible, or result in sensitive and confidential information being compromised, lost or manipulated. Moreover, it could result in Chalmers or its collaborative partners losing creditability and competitive power, and even suffering financial damages.

Research information often consists of information assets that are jointly owned with external parties within a research project or research centre. On many occasions, researchers also handle research information that is owned entirely by external parties.

## Operational and research information

Chalmers' operational information is all information that is owned, produced or maintained by Chalmers staff members (employees, consultants and others participating in Chalmers' operational activities), as well as all information sent to Chalmers and its staff members.

Examples of operational information are:

- Government agency decisions and other internal decisions.
- Information on our public and internal websites and in our newsletters.
- Documents and other data in our operational systems, as well as e.g. in HR systems, Ladok, course databases, accounting systems, and document and administrative process management systems.
- Educational information, such as programme and course syllabuses.
- Student information, such as contact details, study results, and degree certificates and diplomas.
- Contact lists and participant lists for meetings and events.
- Personnel files and notes from performance appraisals.
- The contents of Office documents (Word, Excel, PowerPoint, etc.) and verbal information.
- Other internal documentation, such as activity plans and documents from projects and investigations.

***Examples of research information are:***

- Measurement data, data from simulations and other project-specific databases.
- Analysis and simulation models.
- Software for solving specific research problems.
- The notes and journals of individual researchers or research teams that describe the development of research results.
- Research publications, both in draft format as well as in submitted and published formats.
- Minutes from meetings and protocols from project meetings and other meetings.
- Research applications, research agreements and project plans.
- The content of Word and Excel files, as well as verbal information.

## 2. Responsibility

Each staff member (employee, consultant and others working with Chalmers operational activities) is responsible for handling information assets and IT resources in accordance with these regulations. This also includes all operational information and research information. The responsibility also includes the classification of all information (see separate section).

Each staff member is obliged to report incidents related to the management of operational or research information to the Chalmers Servicedesk (support@chalmers.se). Examples of incidents include:

- information losses
- unintentional dissemination of information
- hacking in Chalmers' IT resources and systems
- theft of computer or other equipment

Line managers and other operations managers shall inform their subordinates about the requirements in these provisions, and monitor compliance with them.

Line managers and other operations managers are also responsible for ensuring their subordinates have access to suitable support and aids as well as the right competence to perform their work tasks.

***The following applies for research:***
Project managers, centre directors and others responsible for the research are responsible for informing their subordinates about the requirements in these regulations, and monitoring compliance with these regulations within their areas of responsibility. They are also responsible for ensuring those involved in the respective project or centre have access to suitable support and aids as well as the right competence to perform their work tasks.

## 3. Classification of information

The information must be classified based on its function and significance for operations, as well as the potential consequences of the information ending up in the wrong hands, being corrupted or disappearing. The classification model is based on the information security aspects *confidentiality, integrity* and *availability.*

Important criteria in the classification include financial value, legal requirements, and general significance to Chalmers' brand and business relationships.

It is important to bear in mind that the classification levels may vary over time. For example, research findings have great requirements for confidentiality and integrity until they are published, in the same way that an annual report has a high integrity factor when the time for financial statements approaches. It is also extremely important that IT systems containing information about Chalmers' education offering (courses and programmes) are available and show correct information during application periods.

### Determine information class

In order to determine which information class an information asset belongs to, the asset must be assessed based on the three information security aspects. Based on the assessed value for each factor C-I-A, it is the highest value that determines the *entire* composite level of the information asset.

For example, if our C-I-A results are *2-3-1*, the information should be assigned information class 3 and managed accordingly.

*Classification based on confidentiality*

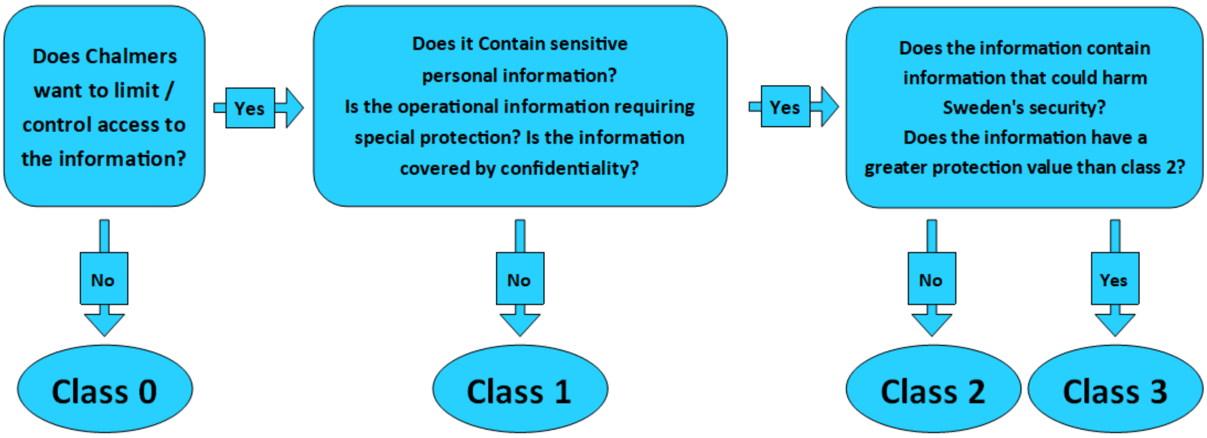
Does Chalmers want to limit / control access to the information?
Yes
Does it Contain sensitive personal information? Is the operational information requiring special protection? Is the information covered by confidentiality?
Yes
Does the information contain information that could harm Sweden's security? Does the information have a greater protection value than class 2?
No
No
No
Yes
Class 0
Class 1
Class 2
Class 3

*Table 1 – Examples of information assets based on confidentiality*

| | |
|---|---|
| **Class 0** | Information presented publicly on the web, without restrictions. |
| **Class 1** | Internal information that does not contain sensitive personal data and is not classified as confidential, procurement, contract, agreement. |

| | |
|---|---|
| **Class 2** | Sensitive personal data, operational information requiring special protection (logs, user information/data, research data), material defined as confidential. |
| **Class 3** | Passwords, encryption keys, particularly sensitive research data. Information linked to a person with a protected identity. Information that could harm Sweden's security. |

*Table 2 – Potential consequences of deficiencies in confidentiality*

| | |
|---|---|
| **Class 0** | Causes no or insignificant consequences for Chalmers.<br>See “Risk analysis”/Risk model *Level 1 Insignificant* |
| **Class 1** | Causes no or minor consequences for Chalmers.<br>See “Risk analysis”/Risk model *Level 2 Minor* |
| **Class 2** | May result in Chalmers violating legislation or other serious negative consequences for operations.<br>See “Risk analysis”/Risk model *Level 3 Serious* |
| **Class 3** | May result in Chalmers violating legislation or other very serious negative consequences for operations.<br>See “Risk analysis”/Risk model *Level 4 Very serious* |

## *Information management – confidentiality classes 0–3*

### Confidentiality class 0, public information

- Access to systems where the information is stored shall be needs-driven, restricted and logged.
- The information may be stored on the workstation’s local hard drives, file servers as well as removable media, telephones or tablets without restrictions.
- The information may be transmitted electronically, e.g. by email or web, without encryption being required.
- The information may be made available for external access.
- The information may be stored in cloud services or equivalent where Chalmers has an agreement.

### Confidentiality class 1, general information

- Access to systems where the information is stored shall be needs-driven, restricted and logged.
- A data processor agreement must be in place in order for personal data to be stored and processed by an external party, for example in a cloud service.
- The information may be stored on the workstation’s local hard drives, file servers as well as removable media, telephones or tablets without restrictions.
- The information may be transmitted electronically, e.g. by email or web, without encryption being required.
- The information may be made available for external access with identification of the user. The information may be stored in cloud services or equivalent where Chalmers has an agreement.

**Confidentiality class 2, highly confidential information**

- The information may be stored on work computers and Chalmers' file storage services.
- The information may be stored on contracted cloud services, but must be password-protected (Office's built-in password function with strong password is acceptable).
- The information may be stored on removable media, telephone or tablet owned by Chalmers, provided it has an encrypted file system and is handled in a secure manner.
- Access to systems where the information is stored shall be needs-driven, restricted and logged.
- Access shall be protected by a strong password as specified in the general recommendations.
- Communication (e.g. by email and the web services) shall not be in plain text, but must instead be transport encrypted using approved solutions, e.g. VPN or web solutions with TLS (https).
- Computers, smartphones and tablets that can access, store and process this information shall comply with the IT department's security requirements. For example, operating systems and related software shall be updated and there must be malware protection.
- The physical handling of information assets labelled confidential must be done with care, and such assets must not be left out where unauthorised persons can access the information.
- When using open public networks (e.g. free, open WiFi at cafés, hotels, trains, buses, etc.), VPN must be used.
- The information may be processed in other approved project and collaborative solutions. Please contact Chalmers' Information Security Coordinator for information or to obtain approval for a solution.
- The processing of information assets in services or IT systems is not permitted in cases where Chalmers or its collaborative partner does not have an approved agreement for use.
- The processing of information assets on privately-owned hard drives, USB memory sticks, telephones or computers is not permitted.
- Calls in public environments regarding information assets belonging to *confidentiality class 2* (e.g. personnel matters, tenders, etc.) must be avoided.
- Information may only in exceptional cases be sent by email, but on such occasion must be encrypted with a strong password.

**Sensitive personal data**

- Where applicable, shall be processed with great caution
- All processing must be reported in advance to the Data Protection Officer.
- May only be processed and stored on a computer with an encrypted file system or file server.
- May not be transferred to or stored outside of the EU/EEA or countries without adequate security mechanisms. Contact dataskydd@chalmers.se if you have any questions.

### Confidentiality class 3, secret information

Information in confidentiality class 3 requires special security measures. These measures are not necessarily the same for all information belonging to confidentiality class 3, but must instead be designed specifically for the respective information asset. A risk and vulnerability analysis shall serve as the basis for designing the correct security measures. The Risk and Security function can help with this work.

## *Classification based on integrity*

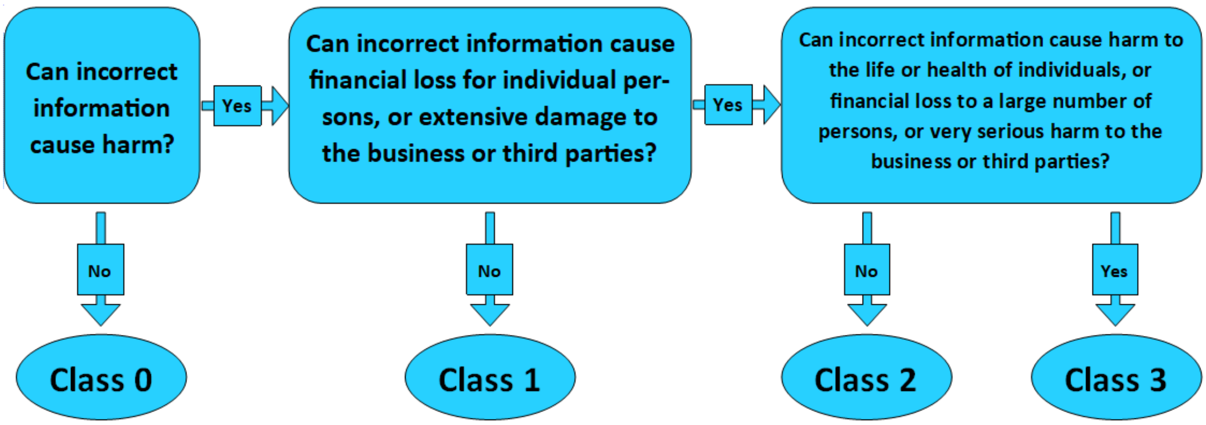
Can incorrect information cause harm?
Yes
Can incorrect information cause financial loss for individual persons, or extensive damage to the business or third parties?
Yes
Can incorrect information cause harm to the life or health of individuals, or financial loss to a large number of persons, or very serious harm to the business or third parties?
No
No
No
Yes
Class 0
Class 1
Class 2
Class 3

*Table 3 – Examples of information assets based on integrity*

| | |
|---|---|
| **Class 0** | - |
| **Class 1** | General information to external users, internal/external communication by email |
| **Class 2** | Research data, scientific software, publications, user groups, personnel matters, logs, bookkeeping materials, original copies of agreements, sensitive personal data |
| **Class 3** | Passwords, firewall rules, particularly sensitive research data |

*Table 4 – Potential consequences of deficiencies in integrity*

| | |
|---|---|
| **Class 0** | - |
| **Class 1** | Causes insignificant or minor consequences for Chalmers.<br>See “Risk analysis”/Risk model *Level 2 Minor* |
| **Class 2** | May result in Chalmers violating legislation or other serious negative consequences for operations.<br>See “Risk analysis”/Risk model *Level 3 Serious* |
| **Class 3** | May result in Chalmers violating legislation or other very serious negative consequences for operations.<br>See “Risk analysis”/Risk model *Level 4 Very serious* |

## *Information management – integrity classes 0–3*

**Integrity class 0 and 1**

- Original information shall be stored using approved solutions with a secure backup function with procedures for testing and restoring.

**Integrity class 2**

- Original information shall be stored using approved solutions (see intranet) with a secure backup function.
- The information shall be synched with Chalmers' storage services (e.g. file servers and procured cloud storage) to ensure proper backup. Alternatively, a procured storage service of a collaborative partner may be used.

**Integrity class 3**

Information in integrity class 3 requires special security measures. These measures are not necessarily the same for all information belonging to integrity class 3, but must instead be designed specifically for the respective information asset. The Risk and Security function can help with this work.

As a rule of thumb, a risk and vulnerability analysis is always required as a basis for designing correct security measures.

## *Classification based on availability*

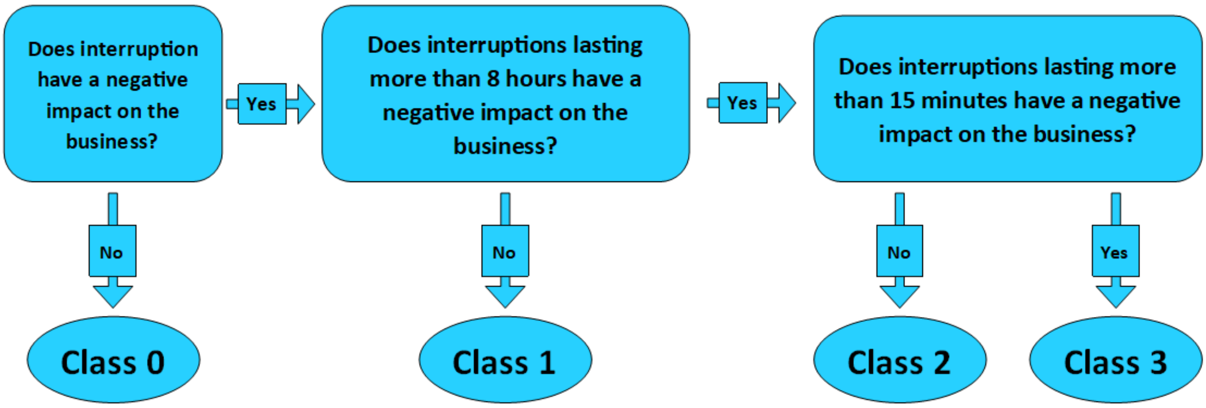
Does interruption have a negative impact on the business?
Yes
Does interruptions lasting more than 8 hours have a negative impact on the business?
Yes
Does interruptions lasting more than 15 minutes have a negative impact on the business?
No
No
No
Yes
Class 0
Class 1
Class 2
Class 3

*Table 5 – Examples of information assets based on availability*

| | |
|---|---|
| **Class 0** | - |
| **Class 1** | HR systems, financial data, payroll lists, logs |
| **Class 2** | Operational diary, AD, file server, study-related information during the application period |
| **Class 3** | *Certain infrastructure that delivers information systems meets criteria for Class 3* |

*Table 6 – Potential consequences of deficiencies in availability*

| | |
|---|---|
| **Class 0** | - |
| **Class 1** | Causes insignificant or minor consequences for Chalmers.<br>See "Risk analysis"/Risk model *Level 2 Minor* |
| **Class 2** | May result in Chalmers violating legislation or other serious negative consequences for operations.<br>See "Risk analysis"/Risk model *Level 3 Serious* |
| **Class 3** | May result in Chalmers violating legislation or other very serious negative consequences for operations.<br>See "Risk analysis"/Risk model *Level 4 Very serious* |

*Information management – availability classes 0–3*

**The management of and responsibility for IT systems, information carriers in the IT infrastructure and other infrastructure is handled within Chalmers' administrative organisation and is regulated individually based on their perspective.**

## 4. General information security requirements

All equipment that handles operational information must be protected against unauthorised access and damage. Computers, smartphones, tablets and other devices that have access to, store and handle Chalmers' information (this concerns both regular operations and research information) must meet Chalmers' security requirements.

Chalmers-owned equipment that is not configured with CDA is designated *Non-CDA*, but must meet the same security requirements as the corresponding CDA platform. It the user's duty and responsibility to know and maintain the security level.

### Password

- Computers and other systems and devices shall be protected by a strong password. A strong password is one containing a minimum of 10 characters and consisting of a mixture of letters, numbers, lowercase, uppercase and special characters.
- Passwords for Chalmers' IT resources or services must be unique and not used for other IT systems or external services. This way, Chalmers is not at risk of being affected if such external services are hacked.

### System security and protection against malware

- There shall be procedures for backup, restoring as well as testing and verifying such.
- Operating systems and related software must be kept updated.
- There must be protection against malware.
- Knowingly connecting equipment infected with a computer virus or other malicious software to Chalmers' IT resources is expressly prohibited.

## Mobile devices

- Telephones and tablets shall be password-protected by a password of at least six characters. On mobile telephones and tablets, Chalmers-approved solutions for biometric identification with fingerprint or facial recognition shall be used instead of a password (e.g. Touch ID and Face ID on Apple iPhone and iPad).
- Mobile device users must protect the device with suitable screen lock (6-character PIN code, complex pattern, facial recognition or fingerprint).
- Computers, smartphones, tablets and external storage devices shall have an encrypted file system. As standard, the Chalmers Computer Workplace (referred to as CDA) uses an encrypted file system for Window 10, macOS, Android phones or Android tablets. iPhone and iPad have an encrypted file system upon delivery from Apple.

## Storage and management

- The storage of work-related material should normally take place mainly on Chalmers' recommended solutions (e.g. computers, file servers, contracted cloud services). If this is not possible, the user is responsible for ensuring that the information is stored securely, and that the information is backed up. If you have any questions, please contact the Chalmers Servicedesk.
- The archiving and purging of Chalmers' information assets shall take place following the University's established rules for this. If you have any questions, please contact the registrar: registrator@chalmers.se.

## Documentation

- The object/system owner is responsible for ensuring that system documentation is available and that it is updated and current. It should include (list is not exhaustive):
  - Interrelations and dependencies between systems
  - Procedures for system maintenance
  - Procedures for backup & restoring
  - Procedures for change management and system development
  - Registration of hardware in appropriate inventory lists

## Incidents

- When outside the regular office environment, Chalmers' IT equipment must be stored out of sight, for example in a wardrobe or lockable cabinet, when not in use to minimise the risk of theft and loss of information.
- If a user discovers or has reason to suspect a security breach or misuse of Chalmers' IT resources, they must report this immediately to the IT department's Incident Response Team (IRT) via abuse@chalmers.se.

## Miscellaneous

- Only open attachments or click on links in email if you trust the sender.
- Remember to be discreet if discussing sensitive information with colleagues or by phone when in public spaces.

- Be restrictive with USB sticks and other similar freebies/giveaways that you can get at trade shows and do not use these in your work computer. They could contain malware or other harmful items. Contact your procurer if you need a USB memory stick.
- The user must ensure that the screen lock is activated on their computer or other devices if they are left unattended.

## 5. Acquisition of IT components and hardware

The IT department is responsible for drawing up and submitting recommendations for the hardware must suitable for the general operations at Chalmers. Chalmers' standard solutions are designed to handle most cases and contexts related to the handling of information assets, regardless of protection value, according to the requirements of these regulations.

These recommendations and examples of standard hardware can be found on Chalmers' intranet. If there are specific requirements or requests beyond the normal recommendations, contact the procurement managers at the IT department.

If deviation from recommended solutions is necessary, the operations manager is responsible for conducting a risk analysis in consultation with the Risk and Security function before a decision on use is made by the Director of IT.

## 6. Information security in research and operational projects

Information security is an important component in project work. Here is some general advice to consider when planning and starting a project. These are relevant for research projects as well as internal operational projects.

- Who owns the information assets
- Who should have access to the information assets
- Should the information assets be shared internally/externally
- If access to electronic resources like licences, software or databases is included in the project, there must also be clear rules for the use of these. If you have any questions, please contact the IT department.
- Where will the information assets be stored
- What security levels the information assets require
- Are there specific laws that affect management of the information assets
- Identify requirements for IT
- Carry out a risk analysis to identify any information security risks and define necessary security measures
- If the processing includes personal data, notification of this must be sent to the Data Protection Officer (dataskydd@chalmers.se)
- At the end of the project, the information must be archived and purged (this includes information stored in cloud services).

# 7. Regulations for employee use of Chalmers' IT resources

These regulations apply to anyone who is employed or has an employment-like form at Chalmers or equivalent, for example consultants, industrial doctoral students and GU employees working at Chalmers.

Regulations for students are addressed separately in the document: Regulations for student use of Chalmers' IT resources (C 2020-0459).

Chalmers' IT resources are intended to be used in and for Chalmers' mission to provide education, research and related administration, as well as for collaboration with the surrounding society, referred to as third stream activities.

The term "Chalmers' IT resources" refers to, for example (list is not exhaustive), mobile devices, computers, computer networks, IT services, information assets, and electronic resources such as licences, software and databases.

## Use and management of Chalmers' IT resources and information assets

Chalmers' IT resources may not be used for the dissemination of information:

- Which violates applicable law, such as incitement against ethnic groups, child pornography offenses, unlawful depiction of violence, libel, harassment, data breach or copyright infringement;
- Which is regarded as political, ideological or religious propaganda;
- Which violates the provisions of the Personal Data Act on personal privacy;
- Which may otherwise be perceived as violating and offensive;
- Which is for commercial activity through the marketing of products or services that are not approved by Chalmers;
- Which in some other way can disrupt Chalmers' IT operations.

### Access rights

- Use of Chalmers' IT resources or networks for which you do not have access rights is prohibited.
- Any attempt to obtain higher access rights to Chalmers' IT resources than you are entitled to is prohibited.
- Use of Chalmers' IT resources to acquire access rights you are not entitled to in other systems is prohibited.

### Use

- Chalmers' IT resources are intended for employees or equivalent, and may not be made available or lent out for private use to family members, acquaintances or others.
- Use of Chalmers' IT resources in a way that could harm Chalmers' name, standing or good reputation is prohibited.
- Chalmers' IT resources are primarily intended for work-related use. Use of Chalmers' IT resources for private purposes is permitted to a limited extent provided that it does not interfere with work, violate other regulations, or expose Chalmers to unnecessary risks.

## Equipment & security

- All computers and other equipment (mobile telephones, e-readers or tablets, computers, etc.) that are connected to Chalmers' network must satisfy a good level of security (which includes a functioning antivirus, firewall and security-updated operating system), regardless of who owns them and where they are located.

## Storage and management

- Documents that may contain material of information class 2 or a higher security level must be handled carefully and in a secure manner. They may not be left out unattended, but must rather be stored in locked spaces, like a filing cabinet. A locked office is not sufficient protection.
- Removable storage media (USB stick, external hard drives or the like) containing Chalmers' information assets must be handled with care and not be left unattended.
- It is permissible to perform work with information belonging to information class 2 in public environments, such as a café or hotel, or when travelling (train, flight or the like), but remember to do so in a way that prevents unauthorised persons from accessing the information, for example by "peeking" at the screen.
- Sensitive information (information class 2 and higher) may only be saved on removable storage media (USB stick, external hard drives or the like) in exceptional cases, and must be encrypted/password-protected to prevent unauthorised access to the data.
- Contact the Chalmers Servicedesk for procedures and the process for destroying used storage media and IT resources

## Encryption

- When encrypting, passwords must be complex and chosen with care, and the backup copy of encryption keys must be stored in a secure place to prevent data loss.

## User accounts and passwords

- Access rights to Chalmers' IT resources are personal and may not be given to another party to use.
- The owner of the respective IT system is responsible for routine and regular access rights management (revision, purging and access rights levels)
- Do not disclose or share your password to anyone else.
- Do not ask anyone else to give you their password.
- Do not use anyone else's personal login details, even if they shared their login information with you.
- The password must be at least 10 characters long and contain at least four alphabetic characters (A-Z or a-z. Not ÅÄÖ/åäö), one number and one punctuation mark. See rules from PDB: https://pdb.chalmers.se/PDB4Web/views/AboutPasswords.jsf
- Passwords must be changed promptly if there is reason to believe that another party may have gained access to it.
- Non-personal passwords to Chalmers' IT resources (e.g. root password, login details to servers or other administration passwords) must be secured against unauthorised access or unauthorised use and at least two copies must be saved, digitally and/or in paper format.
- Use of a password manager for the storage and management of personal passwords is permitted. The master password for the password manager must be complex, hard to guess, and follow the previously defined content requirements.

## Remote work

- When working remotely or using Chalmers' IT resources outside of the campus, good information security must be practiced. Always use Chalmers' equipment and services when possible.
- Only use the software recommended by Chalmers. Skype for business, Zoom and Microsoft Teams are available for e-meetings and distance learning.
- When using public or external WiFi networks, the connection must be secured with a VPN.
- Draw a line between private life and work – Avoid allowing family members to use Chalmers-owned equipment and try to minimise private use.
- Working from home can expose sensitive information in a completely different way than if you are sitting at your regular workplace.
- When planning travel outside of Sweden/the EU, a risk assessment must be performed based on what equipment you are taking along and what systems you will connect to on site. Some authorities also make recommendations regarding information security and the transport of information to and from specific countries.

## Email

A Chalmers email address is intended and permitted for internal and external communication. Some use of a Chalmers email address for private purposes is also allowed, provided it does not interfere with work or expose Chalmers to unnecessary risks.

- Use of a Chalmers email address for political or commercial purposes is not permitted.
- Incoming email must always be handled in accordance with applicable legislation.
- Information assets classified as *highly confidential information* or *secret information* may not be sent in plain text but must instead be encrypted using a suitable method. Contact the Chalmers Servicedesk if you need advice.
- The use of automated rules for forwarding certain email is permitted, but Chalmers employees may not automatically forward all email to an email service outside of Chalmers' procured offering (C 2019-0537).

## Cloud services

- Chalmers' information assets may only be stored in cloud services or equivalent that Chalmers has contracted with, and thus not via private accounts and licences. Contact the Chalmers Servicedesk for more information about which suppliers and services are available.
- If collaborative partners have licences in systems or services with providers that differ from those used by Chalmers, it is permissible to store and process Chalmers' information assets in these. The management of information assets must follow Chalmers' standard regulations.
- If possible, try to send direct links to work-related material in the cloud service instead of sending files by email.
- The installation of cloud service synchronisation software with Chalmers' licences on privately, non-Chalmers-owned equipment is not permitted.
- The owner of a folder must ensure that only authorised persons have access to the material and that access rights are purged as necessary.
- At project end, information stored in cloud services must be archived and purged. Contact the Archives and registrar for more help and more information.

- Information assets classified as information class 3 may not be managed in cloud services. Contact the Risk and Security function for more information.

## 8. Administration of user accounts

The process for creating a computer account for new users at Chalmers is automated. When a person has an active association or affiliation to Chalmers, an account is automatically created in the Persondatabasen (PDB).

The user account forms the basis for access and, in some cases, access control for IT resources and premises at Chalmers, and is an important component of the protection of Chalmers' information assets.

- In order to access their computer account, the user must retrieve a scratch card with password.
- Administrators authorised to assign scratch cards are appointed by the head of department/equivalent and must undergo compulsory training.
- Use of an "agent" to change or set new passwords is not permitted.

## 9. System administrators

The term system administrator refers to persons granted higher access rights than regular users.

### Special obligations and responsibilities

- Dedicated administration accounts or other accounts with elevated rights shall not be used except when the work tasks require such.
- A system administrator has a duty to maintain confidentiality in relation to data and information they learn through their role as system administrator.
- A system administrator shall inform their manager or Chalmers' IRT organisation if they suspect security deficiencies or suspect that an IT security incident has occurred. They must also follow the applicable incident procedures. If the incident involves personal data, this must also be reported, for example, using the form on Chalmers' intranet. Contact the Chalmers Servicedesk if you need help reporting.
- If a system administrator discovers that a user is using Chalmers' IT resources in a manner that violates applicable regulations, that user must be made aware of this.
- In the event of serious or repeated violation, Chalmers' IRT organisation must be informed.
- A system administrator must have good knowledge of the current guidelines for Chalmers' IT resources and information security.
- A system administrator should use the existing solution for two-factor authentication if this is technically possible and the systems allow this.

The system administrator's duty to maintain confidentiality as specified above does not limit the system administrator's rights and obligations under the Freedom of the Press Act and the Public Access to Information and Secrecy Act.

### Powers

- A system administrator has the right to monitor the part of the resources they are responsible for and to intervene without warning if this is necessary to be able to handle the daily operation of the system and to perform troubleshooting.
- In the event of an emergency, a system administrator has the right to quickly and without warning limit the availability and use of IT resources or infrastructure in order to minimise any damage.

## 10. Information security incidents

Information security incidents may be subject to mandatory reporting to external authorities such as the Swedish Civil Contingencies Agency or the Swedish Data Protection Authority due to the extent of the incident. It is important that all incidents are investigated as soon as possible after they have occurred in order to get a clear picture of the situation and what can be improved. The person appointed as incident manager is responsible for convening meetings for debriefing and lessons learned.

### Monitoring and measures in case of violation

- To ensure a high level of security, network traffic and stored data may be logged and monitored, and may be investigated for possible violations of applicable laws and user guidelines.
- Logs are saved and archived in accordance with applicable laws and regulations on purging and archiving.
- Computer and electronic resources connected to Chalmers' networks are systematically scanned regularly for known vulnerabilities.
- Violations of these guidelines may be reported to the line manager/head of department or equivalent for disciplinary measures. Suspected violation of law will be reported to the police.
- In the event of serious breaches of applicable information security guidelines, investigation of suspected irregularities or law violation, IT equipment owned by Chalmers may be seized by the IRT/IT department for further review and preservation of evidence.
- A manager may temporarily suspend a mismanaged or misused IT resource with immediate effect.

### Investigation of computer incidences

The IRT is organised under the Infrastructure unit of Chalmers' IT department.

- The IRT has the right to monitor use of systems and access network traffic in order to seek out weaknesses/deficiencies in systems or on behalf of the Risk and Security function.
- The IRT has the right to evaluate and test security in Chalmers' IT environment by, for example, systematically scanning for vulnerabilities.
- The IRT has the right to use log files for internal investigations, and logs may also be disclosed to the Swedish Police.
- The IRT has the right to gain access to Chalmers-owned IT equipment for investigative purposes if there is reason to suspect it is being used in violation of user rules.

- The IRT only provides investigation-related information to authorised personnel, usually security coordinators, information security coordinators or persons known to be investigating the incident.

## 11. Personal data processing

Chalmers handles personal data within the framework of its operations and in accordance with applicable laws and regulations. Line managers and other operations managers are obliged to know the extent to which sensitive personal data is handled within the organisation and by its employees. For more detailed information, please see the separate privacy policy at chalmers.se.

## 12. Archiving and the dissemination of information

Chalmers' operational information shall be archived as soon as the final version has been drawn up. The archiving of electronic documents shall preferably be done using Chalmers 360, but can also be done in other operational systems such as Canvas, Studieportalen, VIS and Raindance for later transfer to Chalmers' e-archive.

Agreements, protocols and decisions and other documents with signatures are archived as original paper copies in Chalmers' central archive, even though electronic copies shall always be registered in Chalmers 360 for the sake of availability. Destruction is only permitted if in compliance with applicable regulations and the application decisions taken by Chalmers.

***The following applies for research:***
All research publications produced at Chalmers University of Technology, as well as doctoral and licentiate degree dissertations, conference contributions, journal articles and reports shall be published in the Chalmers Publication Library (CPL) in accordance with Chalmers' Open Access policy.

### Principle of Public Access to Official Documents and the dissemination of information

Chalmers University of Technology AB and the Chalmers University of Technology Foundation are subject to the Principle of Public Access to Official Documents. Chalmers is named in the *Public Access to Information and Secrecy Act*[1] *(2009:400)* (OSL), which regulates the public's right to access documents at an authority. This means that public documents stored at Chalmers are to be disclosed on request, after the customary confidentiality assessment. Examples of public documents are:

- Email at the authority.
- Official decisions and other decisions.
- Internal investigations and reports.
- Agreements with external parties.

[1] **OSL 2009:400 Chapter 6, § 4**: *An authority shall, at the request of an individual, provide information from a public document kept by the authority, unless the information is classified or would impede the proper conduct of the work.*

According to the Public Access to Information and Secrecy Act, documents containing classified information must always be registered and archived, which takes place in Chalmers 360. For support in this process, contact the Archive and Registrar.

If you would like information on how to handle your specific documents, our most common document types are listed in Chalmers' operations-based archiving report. It is currently available in the 2C8 tool.

## 13. Collaboration with industry/other external partner

The format and forms of collaboration with an external party as well as the sharing of information assets must be defined right from the start-up procedure. The aim is to clarify areas such as responsibilities, where the information is stored, which suppliers and services are involved, and how the information assets will be handled at the end of the collaboration. It may be the case that collaborative partners have licences with other suppliers than those used by Chalmers, which is important to keep in mind when sharing information assets.

Before any agreement containing confidentiality requirements is signed, Chalmers' Legal counsel must be consulted.