GHENT
UNIVERSITY

INFORMATION SECURITY

TECHNICAL AND ORGANIZATIONAL MEASURES AT GHENT UNIVERSITY

Non-confidential, version dd. 17 February 2022.

Table of contents

1 Introduction

This document provides an overview of a number of strategies and measures followed within Ghent University (UGent) in order to optimally guarantee the security of data and information. It lists measures Ghent University takes to guarantee the integrity, availability, confidentiality, and cyber resilience, as well as the non-repudiation, the authenticity of information and the auditability of information processing systems. This is a non-exhaustive overview, meaning that not all the measures taken are listed in this document.

2 General Security Policy and Organization of Information Security

2.1 Information Security Policy

Ghent University has a modular data protection and information security policy. The various modules of this policy have been built up gradually in recent years. The policy as a whole is assessed annually and updated where necessary.

The policy has been adapted to the context of Ghent University, it is in accordance with the provisions of the applicable legislation and relevant decrees, and of the General Data Protection Regulation.

Ghent University's information security policy includes:

- procedures for protecting the information data contained in electronic messages
- procedures for protection against data loss
- malware protection procedures (updated antivirus, firewall, ...)
- a user access management policy that restricts access to systems and services to authorized users and prevents unauthorized access
- an appropriate password policy
- procedures for protecting access to the servers
- procedures for protecting access to the network
- procedures for the protection of the workstations
- procedures regarding the classification of information data according to their value or their critical or sensitive nature in the event of modification or unauthorized disclosure, and regarding the consequences of the classification

The IT infrastructure for digital preservation of highly confidential data is protected against any known risk of individual intrusion and against unauthorized access to the information it contains. Any form of individual intrusion or unauthorized access to the files is detected. In the event of such a detection, the necessary countermeasures, including alarms, come into immediate effect. This security system functions independently of the computer systems used for digital storage of these highly confidential data.

2.2 IT Security Officer

Ghent University has appointed an IT Security Officer who is responsible for IT security and for information and data protection. The IT Security Officer is a permanently invited expert in Ghent University's ICT Committee and is a member of the Privacy and Data Protection Committee. The IT Security Officer reports to the Director of the ICT Department.

2.3 Data Protection Officer

Ghent University has appointed a Data Protection Officer. The Data Protection Officer is responsible for internal supervision of compliance with the GDPR and national data protection regulations. To this end, the Data Protection Officer collaborates with the IT Security Officer and is assisted by a Privacy and Data Protection Committee with representatives from all levels of the university. The Data Protection Officer reports to the Director of the Administrative Affairs Department and to the Vice-chancellor.

2.4 Information Security and Data Protection Responsibilities

Responsibilities of Ghent University staff are documented and published formally in the modular data protection and information security policy.

Important documents are the "Generic Code of Conduct for Personal Data and Confidential Information Processing" and the "Regulations for the Acceptable Use of Ghent University's ICT Infrastructure" (i.e. the Acceptable Use Policy).

2.5 Risk Analysis, Management and Control

Ghent University carries out periodical risk analyses of its security measures and checks their compliance with the various information security procedures.

As far as central IT services are concerned, this is the responsibility of the IT Security Officer, in collaboration with the ICT Department and the Data Protection Officer.

General risk management in the field of data protection and IT security is subject to selective audits by Ghent University's Internal Audit Service. Results of such audits are communicated to Ghent University's Audit Committee and the Board of Governors.

As far as the decentralized IT applications are concerned, risk management is a shared responsibility of the IT Security Officer and decentralized IT administrators. Ghent University's modular information security policy provides guidelines for IT administrators and IT end users for information security risk management.

3 Secure personnel policy

3.1 Training Sessions on the Importance of Security and Handling of Personal Data

Ghent University regularly communicates about the importance of information security to all staff and students. Online training modules are made available to staff members. Where necessary, specific training and/or information sessions are organized, for example for new employees.

Ghent University's system engineers (ICT Department) take a thorough training upon recruitment. Additional training sessions are provided at regular intervals to ensure that their knowledge remains accurate and up-to-date.

3.2 Authorizations

Ghent University implements and maintains authentication and authorization management systems to control access to systems containing personal data. Where possible, role-based authorizations are used.

At a minimum, logical access to each information system is secured with strictly personal credentials (username/password). Authentication and authorizations are always based on the information that is present in redundantly designed central repositories (LDAP and AD, partly on-prem, partly in the cloud with AAD in a hybrid setup).

Account granting and authorization is based solely on board-approved rules and is linked directly to primary staff and student management resources. They expire automatically when the individual's statute expires. The rules for correct use of the personal credentials and account are laid down in Ghent University's Acceptable Use Policy.

3.3 Segregation of Duties

Ghent University applies segregation of duties as much as possible to prevent individuals from gaining access to data they do not need to carry out their duties. This is technically enforced where possible.

4 Physical security of work and office space

Ghent University restricts access to work and office space where personal data or confidential information is processed pursuant to its mandate. Where necessary and based on risk analysis, access is strictly limited to identified and authorized individuals. Burglary protection and/or badge readers are installed to prevent unauthorized access where necessary.

Managing and securing physical access to Ghent University premises is the responsibility of the Security Coordinator at Ghent University's Emergency Centre.

5 Data Centre Security

5.1 Introduction

The data of Ghent University's various central server and storage systems is part of information systems in two separate data centres located in Ghent. The primary data centre is located at Campus Sterre, the secondary data centre at Campus Ardoyen.

5.2 Physical Data Centre Security

Physical access to our own data centres is strictly managed and controlled, and secured according to industry standards, including video surveillance and intruder alarms.

Access to the data rooms is secured by badge readers. The server rooms in each data centre are only accessible to authorized Ghent University system engineers. If external parties need physical access to one of the data centres, this is always done in the presence and under the supervision of a Ghent University system engineer (ICT Department). Badges are issued in accordance with a strict physical identification process, and each staff member must register in person to obtain their badge. All entrances can be read centrally so that entrance to the rooms can be checked at any time.

Each data centre is equipped with fire extinguishers. In the event of a fire, the fire can be extinguished with minimal impact on the IT systems. The temperature and humidity in the rooms is measured continuously. The system sounds the alarm when certain threshold values are exceeded.

For applications and data that are hosted in external cloud systems, an analysis is made beforehand to determine whether the associated risks are sufficiently under control and acceptable.

5.3 Redundancy

All facilities and services in our own data centres are protected against unforeseen failures with sufficient redundancy.

Each data centre is equipped with professional installations to guarantee continuity of power supply (by means of UPS installations and diesel generators) and cooling (by means of redundant cooling machines and fans).

In addition to the primary data centre, Ghent University also has a fail-over data centre. The most critical information systems are redundantly designed over the two data centres, so that in the event of a failure of a single system or even the loss of an entire data centre, the operational functioning of various crucial services at Ghent University can still be provided.

5.4 Disaster Recovery Planning

Ghent University has disaster recovery plans to minimize downtime in the event of disasters involving the IT infrastructure in the central data centres. The disaster recovery plans are updated regularly, and the emergency scenarios are in principle tested and assessed annually.

A dual backup and restore strategy, based on snapshot technology and data replication on the one hand, and daily backup copies on the other, guarantees that data loss in the event of a disaster in one of the centres is kept to a minimum. Backups are taken on specific backup storage systems. An identical copy of all backup data is kept in both data centres.

6 Internal network security

Ghent University's internal network (UGentNet) is highly compartmentalized and equipped with advanced control mechanisms (firewall, intrusion detection & prevention) that protect the internal network appropriately against unauthorized access and unwanted actions from outside. To this end, Ghent University collaborates with its Internet Service Provider Belnet.

Up-to-date encryption protocols are used for the wireless networks to provide maximum protection for the transferred data.

7 Security of data at rest

7.1 Data Encryption

Ghent University’s data storage policy stipulates that digital personal data and confidential information must be stored on centrally provided storage options. External cloud services must not be used to store high-risk data, unless the data is encrypted beforehand (i.e. client-side) in a secure and reliable manner with cryptographic tools.

7.2 Antivirus and Security Updates

Fixed and mobile user equipment is protected by up-to-date antimalware tools. Ghent University provides its central IT systems and user equipment with the latest security updates under central management. These are followed up as closely as possible and installed according to a reliable patch management process.

7.3 Malicious Software

Ghent University performs anti-malware checks to prevent malicious software from causing damage, e.g. gaining unauthorized access or making access to its own data impossible (protection against ransomware).

7.4 Access Logs

ICT system administrators log and monitor access to Ghent University's ICT infrastructure to ensure its proper functioning and to detect and prevent abuse. The level of detail is no more and the retention time no longer than necessary to achieve this goal.

Depending on the type of data or information and their degree of confidentiality, the logging is less or more detailed. For critical information systems, access and actions are logged extensively. Logging information is confidential and can only be released after a formal request accepted by university management (e.g. a court order).

8 Security of Data in Motion

Ghent University uses up-to-date encryption protocols (TLS, HTTPS, VPN) for the transmission of data inside and outside the Ghent University network.

9 Ghent University Account Security

Ghent University accounts are protected by a password that must be renewed at least annually. The passwords must have a certain level of complexity. These requirements are also enforced technically. All Ghent University accounts are secured with an additional multifactor authentication.

10 IT Systems and Server Security

Ghent University applies risk management to the security of all its IT systems. Critical systems and critical applications are subject to a regular safety test by an independent third party. The requirements for data and systems protection are also analysed and specified where necessary in collaboration with IT suppliers.

11 Incident Management

All centrally managed information systems are monitored continuously. The ICT Department has a 24/24 and 7/7 on-call service to be able to intervene immediately in the event of a malfunction.

For the triage and handling of incidents, the ICT Department has developed a scenario for all IT incidents, including those involving personal data. When Ghent University acts as a personal data processor, and in the event of a data security incident that has a significant impact on the confidentiality or integrity of that personal data, Ghent University will inform the Data Protection Officer (and any other interested parties) without undue delay.

Incident management is registered and monitored by a central management system. A monthly incident report is drawn up, including every occurrence, their impact and solution, and lessons learnt.

To minimize the chance of incidents, fixed maintenance windows are scheduled to perform the necessary proactive maintenance activities. In case of urgent maintenance work, urgency maintenance windows are scheduled. During such a maintenance window (a group of) systems may be temporarily unavailable. Each maintenance window (and its possible impact) is therefore widely announced throughout the organization (via intranet).

12 Additional Measures

The above elements describe Ghent University's general, centrally co-ordinated IT services security policy. Based on a more detailed risk analysis, additional appropriate measures are taken for specific processing operations on central or decentralized IT infrastructure, in the context of research projects involving personal data or confidential information.