SimCorp

Information Security Policy

SimCorp Group

Version 4.4: Updated May 2022

Contents Page

1. Introduction

SimCorp's internal applications and technical infrastructure are vital to our ability to conduct business. The purpose of this Information Security Policy (the "Policy") is to ensure the accessibility, performance, confidentiality, and integrity of the IT infrastructure and applications.

SimCorp expects employees to behave within the law, to behave responsibly, and to recognize their responsibilities for secure information handling – including keeping information confidential, and maintaining knowledge of our existing information security practices, and general security awareness.

The Chief Information Security Officer and Security Steering Committee are accountable for the Policy which is reviewed and approved annually. Compliance with the Policy will be checked regularly.

1.1. Scope

Information and IT risk in SimCorp is defined broadly. It encompasses not only traditional risk areas such as network and system intrusion, confidentiality breaches, etc., but also loss of productivity due to downtime or staff frustration, and loss of business opportunities.

The Policy covers applications, infrastructure/technical environment and all information stored on electronic media. Information includes not only information owned by SimCorp but also information owned by third parties which SimCorp is responsible for protecting. Examples of the latter are partner information, customer databases, customer information such as RfP materials, etc.

This Policy applies to all employees of SimCorp without exception, including employees, consultants retained by SimCorp and others whom SimCorp has granted access to its property and IT infrastructure. SimCorp employees may not deviate from the Policy without obtaining prior written approval by the Chief Information Security Officer or head of Group IT. Unless stated directly in the document, this Policy applies to all entities of SimCorp.

2. Physical access control and environmental protection

SimCorp's IT assets must be protected from physical threats, including damage, theft or sabotage. It is therefore important that we restrict the access to SimCorp premises and that we keep track of both employees and visitors.

SimCorp premises include all SimCorp offices as well as our off-site data centres.

2.1. Physical access controls to offices

All SimCorp employees must have an access card or token to enter SimCorp office buildings. The access card must be worn visibly at all times when in an office of SimCorp.

When entering the offices outside of normal business hours and when entering the building during business hours through all doors but the main door, a PIN code will have to be used in combination with the access card or token.

All visitors must be registered at the reception in all units. All visitors in SimCorp premises must be accompanied by a SimCorp employee and the visitor card must be worn visibly at all times.

Main network wiring closets and floor network wiring closets in all entities must be locked and access restricted to relevant IT Operations staff.

2.2. Subsidiaries

Subsidiaries are expected to maintain the level of access control described above, in order to ensure that network wiring closets, IT storage and other essential installations are duly protected. Local exceptions may occur, but these must be documented and approved by the Head of Group IT and Information Security Officer.

2.3. SimCorp data centers

SimCorp's co-location data centres must employ security procedures no less vigilant than those of SimCorp. SimCorp must have a copy of the data centre's security policies in its possession at any point in time.

Access to SimCorp's data centre is limited to a number of named employees in IT Operations and administered by the IT management.

2.3.1. Environmental protection of data centers

SimCorp data centers (including co-locations) must have appropriate protection measures against environmental threats including:

- Fire suppression systems
- Smoke detectors
- Protection against flooding (e.g. raised floors)
- Uninterruptible power supply, including surge protection and diesel generators for providing power during prolonged outages
- Temperature and humidity controlled environment, including temperature and humidity monitoring
- 24/7 closed-circuit television (CCTV)

2.4. Clean desk policy

People with access to SimCorp offices, when leaving the desk, must ensure that documents containing any confidential or private information (including client information) are placed in a safe,

secure environment such as a locked desk drawer, filing cabinet, or other secured storage space. Otherwise, these documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.

Client-relevant information written on whiteboards or flipcharts must be removed when no longer needed or when meetings end.

Printouts containing restricted or sensitive information should be immediately retrieved from the printer.

3. Access control to computer systems and electronic media

In addition to the physical access controls, SimCorp needs to have adequate procedures in place to guard against unauthorized access to our technical infrastructure, applications and information.

The confidentiality and integrity of data stored on company computer systems must be protected by access controls, to ensure that only authorized employees with relevant business needs have access.

3.1. Password policy

The following password policy applies to all information systems in SimCorp (servers, end-user devices, application user accounts etc.). All exceptions to this policy must be documented and approved by the Head of Group IT and Information Security Officer.

- Passwords must consist of at least 8 alphanumeric characters and must contain at least 1 capital letter, at least 1 letter in lower case, and at least 1 numerical character.
- The minimum period between password changes is 1 day
- The maximum period between password change is 90 days
- It is not possible to reuse the last 10 passwords
- The account will be locked after 3 unsuccessful logon attempts
- The count of bad logon attempts will be reset after 30 minutes
- An employee who requests a password unlocking or change from Group IT Service Desk, must be prompted to create a new password at the first login after the change.

Additional security policies:

- For smartphones and tablets, a minimum of a -digit pincode is required.
- Two factor authentication is required for access from outside the corporate network, for example when logging on remotely via Citrix
- Two-factor authentication is required for accessing corporate cloud services, e.g. Microsoft 365/Azure, Salesforce, Workday, Cornerstone
- All systems and applications should have Single Sign-On (SSO) configured as preferred method for login purposes

3.2. Administrator accounts

The general administrator password must follow the standards mentioned above. The administrator password may only be revealed to users with business need for access and must under no circumstances be recorded outside password database systems designed to store such information securely.

Administrator accounts to both the infrastructure and applications will undergo regular monitoring, and accounts not used for 90 days must be disabled.

3.3. Access to software and applications

3.3.1. System access

An employee's access to internal applications must be reviewed on a regular basis and access to components, sites etc. will be removed if there is no business need to access them.

In the event of the termination of an employee's employment with SimCorp for whatever reason, the user account must be locked at the end of the last working day. Managers and supervisors must notify Group IT Service Desk promptly when an employee has been terminated from the company and relieved from duties immediately as revocation of user rights in such cases cannot await regular procedures.

The individual employee is responsible for all computer transactions that are made with the User ID and password. The employee must not disclose passwords to others including IT personnel or family members. Passwords must be changed immediately if it is suspected that they have become known by others.

Employees must lock their workstation whenever leaving it out of sight. All workstations must be configured to lock automatically after being idle for maximum of 15 minutes.

3.3.2. Software installation

SimCorp laptops are provided for the employees' use when performing work duties. However, since the devices are also mobile and are expected to be used when working from home or travelling, users are allowed to install software for personal use within the following restrictions:

- Pre-installed SimCorp applications and tools may not be uninstalled, disabled or replaced by the user. Doing so means that work-related functions may stop working. If a PC is used for testing, or other work which requires a standardised setup, the user may not install software, or in other ways change the configuration of the device. Similarly, users may not install software that is not work-related on virtual machines.
- All installed non-SimCorp software must be legal, and the employee is responsible for keeping proof of purchase and/or licenses for installed software. Group IT may request to see these as part of regular monitoring of security and license compliance.
    - No confidential (including client data), sensitive and copyrights data can be shared unless the software or web-based application is approved by Group IT, to ensure that security requirements are setup (e.g. SSO).

- All content on the PC must comply with the other requirements set out in this policy. It is therefore not allowed to store programs or data of a racist, pornographic or otherwise offensive nature.
- No peer-to-peer file sharing tools (e.g. BitTorrent) may be installed, even for sharing of legal software or data.
- No tools for anonymizing or encrypting web traffic (e.g. Tor, Hola etc.) may be used, as they may interfere with our antivirus and anti-malware tools.
- The user is responsible for backing up all personal programs and data on the laptop via cloud-based services - OneDrive (note that company information/files may NOT be copied to cloud services that are not provided by SimCorp)
- No software may be installed on client systems without express prior client approval.

Group IT will regularly monitor installed software on corporate PC's. Serious or repeated breaches of the security policy will be reported to the employee's manager and may result in disciplinary action.

3.3.3. Access to client systems

Client systems and data must only be accessed from SimCorp owned or managed equipment (or remote connection services such as Citrix) which is compliant with relevant SimCorp policies (such as this security policy, and policies regarding software management).

3.4. Fax machine

No information related to XD clients may be transmitted via fax.

4. Computer virus protection

It is SimCorp's policy to protect its assets efficiently against computer virus regardless of the source and how the virus is delivered.

4.1. Protection against computer virus

Host firewalls and continually updated virus detection software must be in place on all servers and clients throughout the company.

Employees must not knowingly introduce a computer threats (e.g. virus, malware, trojan, etc.) to SimCorp's network, computers or any kind of device owned or operated by SimCorp, unless explicitly authorised by the Chief Information Security Officer for testing purposes and with appropriate safeguards put in place.

CD's, DVD's, USB devices, or any other kind of portable storage device of unknown origin must not be introduced to SimCorp's network, computers or any kind of device owned or operated by SimCorp.

5. Separation of networks

SimCorp's production network must only be accessed by SimCorp employees and duly authorized external consultants. No unauthorized computers or devices may be connected to SimCorp's production network.

A separate network for visitor access is available at most SimCorp offices. The visitors' network offers wireless access to visitors and is wired into all meeting rooms. The visitors' network can only access the Internet.

Some SimCorp offices provide access to a special wireless network (network SSID: "SimCorp-BYOD"). for privately owned mobile devices.

Course rooms access a separate course network ensuring that external course participants cannot access the production network.

Testing networks must operate completely independently of production networks, as testing may occasionally involve software that is not authorized for the production network.

6. Cloud services

When using cloud-based vendors to provide IT services for SimCorp, such vendors must comply with this policy in the same manner as any internal system.

6.1. Authentication

For the purpose of authentication, cloud services are considered to be outside SimCorp corporate network, and access must therefore be based on two-factor authentication, in accordance with section 3.1.

6.2. Physical and environmental security

The cloud vendor must provide documentation for the data hosting services used (irrespective of whether they are owned by the vendor our sourced from a third party). Such documentation must include descriptions of the physical access control measures and the environmental protection measures in accordance with section 2.3. The vendor must either provide an annual audit report regarding these services or be available for SimCorp to audit these services.

6.3. Personal information

Personal data as well as other data may be moved to cloud services as part of SimCorp's use of such services. This may involve transfer of data to countries outside EU. SimCorp will ensure that employee's personal data is safe in the cloud by entering into the necessary legal agreements with

such cloud service providers. Where required, the transfer of personal data outside of EU will be communicated to and approved by the relevant domestic Data Protection Agencies.

7. Mobile devices

Employees of SimCorp are using an increasing number of mobile devices such as laptops, smart phones, and USB devices (memory sticks and external hard drives). Common to these devices is that they can be used to carry data and/or to access SimCorp's network. Common is also that the devices are regularly removed from SimCorp premises resulting in an inherent risk of loss or theft. Aside from the value of the device itself, there is a risk that confidentiality of data can be compromised and that unauthorized individuals can gain access to SimCorp's IT infrastructure.

Employees must handle both corporate devices, and private devices containing SimCorp information, with common sense, and in a way that minimizes the risk of loss or theft. If a laptop or mobile phone is lost or stolen, the employee should inform Group IT Service Desk as soon as possible.

7.1. Laptops

Most employees of SimCorp are equipped with laptops. SimCorp has chosen not to limit its employees as to where they can bring their laptop as the company believes its employees are able to safeguard devices allocated to them. All hard drives on SimCorp-owned laptops must be encrypted.

7.2. Mobile phones

Mobile phones used to access SimCorp information must require a PIN code to log on to the mobile phone. Mobile phones must be locked when left idle for more than 5 minutes.

Mobile phones with access to SimCorp information must be encrypted. Any mobile phone configured to access SimCorp's email system will automatically have a security policy enforced that enables encryption. For this reason, SimCorp may choose to limit which mobile operating systems may be used for accessing corporate information. Additionally, SimCorp may require the installation of management software on the mobile phone. Such software will always be configured to operate in compliance with relevant legislation.

Employees must ensure that the mobile phone app's and operating system are up to date.

For information about private use of your company mobile phone please refer to SimCorp's Mobile phone policies.

7.3. Two-factor solutions and remote access

SimCorp-approved two-factor authentication techniques must be used when connecting remotely to SimCorp's IT infrastructure. In addition, they must be used when authenticating to cloud services provided by SimCorp (e.g. Microsoft Office 365).

7.4. USB Memory sticks and other USB devices

USB devices are used for storage and for exchange of data between workstations not interlinked by a network. No confidential or sensitive data (including client data) must be stored on a USB stick or other USB device, unless the device is encrypted. Such encryption will be technically enforced on SimCorp workstations.

7.5. Customer hard drives and customer data

When using external HDD drives for data transportation (e.g. receiving databases from clients for use in testing or trouble shooting activities), care must be taken to protect the data on the hard drive.

Such HDD drives or similar media must be securely wiped before SimCorp sends them to a third party, eliminating the possibility that data is disclosed inadvertently. Further, these devices must be encrypted when containing data.

7.6. Accessing confidential information via mobile devices

All mobile devices which are used to access confidential SimCorp information (e.g. Salesforce.com, Microsoft 365, downloaded documents) must comply with SimCorp security policies. In effect this means that employees may only use their company laptop, and mobile phones, tablets or laptops that are enrolled to SimCorp's Mobile Device Management solution, since these comply with requirements for session timeout, passcode to unlock, encryption etc.

It is not allowed to access confidential information from any other devices, including the employees own private PC (except if using Citrix).

8. Internet and e-mail

Internet and e-mail are invaluable tools in a modern workplace. To ensure that all employees act responsibly while using the Internet and e-mail the following rules have been established:

8.1. Internet Security

Specific types of websites are blocked for access from the company network. Examples of types of blocked sites are:

- Remote access services for personal business
- Peer-to-Peer files sharing services

When using your PC on a non-SimCorp network, the rules above may not be automatically enforced. Employees should use good judgment to ensure that they comply with the rules above, and the rules in section 8.3-8.5, as best possible.

8.1.1. Social Networks / Media

Social networking is often considered a less formal and even 'harmless' way of communicating, and as such many fail to consider that they may inadvertently breach contractual obligations, such as

confidentiality and secrecy policies. For guidance on the use of Social networks and media in SimCorp, please follow SimCorp's Social Media Policy.

8.2. E-mail Security

External e-mails are not necessarily encrypted and there is a risk that e-mails can be picked up and read by third parties. Employees should always keep this in mind when composing the content of external e-mails.

8.2.1. Handling of email account for resigned employees

When an employee leaves the company, the user's account will be disabled, and an Out of Office-reply added to the account, stating that the employee no longer works for SimCorp. The email address will be open for incoming mails in a given period for business reasons, after which incoming mails will be blocked.

If access to the mailbox of a resigned employee is needed for business reasons, this can be granted in agreement with the resigned employee's manager.

8.3. Acceptable use of Internet and e-mail

When accessing the Internet or when sending and receiving e-mails from their company computer employees are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, appropriate and lawful manner. Examples of acceptable use are:

- Using web browsers to obtain business information from commercial websites
- Accessing databases to retrieve and potentially download commercially relevant information
- Using e-mail for business purposes
- Download business relevant documentation
- Personal use of the provided equipment in a way that does not interfere with SimCorp's security posture, or the employees' work tasks

8.4. Unacceptable use of internet and email

Employees must not use the Internet for purposes that are illegal, inappropriate, potentially harmful to the company, the company IT systems, introduce possible risk to corporate data, or counterproductive. Examples of unacceptable use are:

- Broadcasting e-mails
- Conduct personal business using company resources in a manner or scale that interferes with the performance of the employees' work tasks
- Downloading or transmitting any content that is illegal, inappropriate, harassing, or fraudulent

In addition to the rules stated above, SimCorp will maintain and enforce a list of automatically blocked websites, based on security and appropriateness considerations.

8.5. Employee responsibilities

An employee who uses the Internet or e-mail must:

- Be responsible for the content of all text, audio, or images that the employee places or sends over the Internet. All communication should have the employees name attached
- Not transmit copyrighted materials without permission
- Know and abide by all applicable SimCorp policies dealing with security and confidentiality of company records
- To the extent possible, avoid transmission of non-public customer information. If it is necessary to transmit non-public information, employees are required to ensure that information is delivered to the intended recipient and appropriately protected during transmission (i.e., in accordance with client contract terms).

8.6. Ownership of e-mails and SimCorp's access hereto

All e-mail messages created, sent, or retrieved via SimCorp's e-mail system are the property of SimCorp and are regarded as company information.

All e-mails sent and received via SimCorp's e-mail system are stored centrally and will be subject to regular backup.

SimCorp reserves its right to access and open e-mails sent or received by employees of SimCorp for the purposes of

(i) Securing SimCorp's continuous IT operations

(ii) Preventing threatened or remedying actual breaches of the IT-security of SimCorp

(iii) Securing documentation of matters related to SimCorp's business and

(iv) Monitoring the compliance of employees with this Policy.

8.7. Monitoring of Internet Access

SimCorp carries out monitoring and logging of the Internet Access of its employees in order to secure compliance with the acceptable use policy, to prevent threats, and to remedy any actual breaches of the IT security of SimCorp. This monitoring and logging is also enforced when the employee is using a corporate laptop outside the corporate network.

9. Decommissioning of old hardware

Data storage hardware that is no longer used must be either destroyed or wiped in order to ensure that applications and information of the device cannot be used or restored by any unauthorized party. This includes hard drives of decommissioned personal computers and laptops.

If such data wipe is performed by third parties, SimCorp must receive documentation for the performed data wipe (e.g. certificates).

10. Protection of physical devices

It is the company policy to protect computer hardware, software, data and documentation from misuse, theft, unauthorized access, and environmental hazards. In support of this policy, it is the responsibility of each individual employee to keep external storage devices that contain confidential data locked up, when left out of sight.

11. Confidentiality guidelines

As a publicly traded company and as a company operating in a competitive environment SimCorp must ensure that sensitive information is kept confidential until management decide to make it public.

For details, please see the following document Confidentiality Guidelines.

12. Copyrights and license agreement

SimCorp and its employees are legally bound to comply with local Copyright Acts and all proprietary software license agreements. Non-compliance can expose SimCorp and the responsible employee(s) to civil liability and/or criminal charges.

This directive applies to all software that is owned by SimCorp, licensed to SimCorp, or developed using SimCorp resources by employees or vendors.

12.1. Responsibility of Group IT

Group IT must maintain records of software licenses owned by SimCorp. Corporate computers will periodically be scanned to verify that only authorized software is installed.

12.2. Employee responsibility

Employees are responsible for keeping documentation for licenses for any employee-installed software on corporate computers, as described in section 3.3 of this policy.

13. Awareness, enforcement and monitoring

13.1. Employee awareness training and testing

SimCorp will regularly and at least on an annual basis conduct training in Information Security for all employees. The training may be tailored specifically to the employee's area of responsibility or be of a more general nature.

As part of the training, and to assess the effectiveness of the training programme, SimCorp may occasionally conduct awareness surveys, in which employees' ability to identify e.g. harmful emails, will be tested by sending simulated versions of such e-mails. For technical reasons it may be necessary to temporarily store data about individual users' responses, but no records of individual employee responses will be permanently kept.

13.2. Security event reporting

If an employee detects a security threat or breach, the employee is obliged to report immediately to the Information Security team or Group IT Service Desk.

13.3. Monitoring of systems and networks

Employees should observe and be aware that it is legal to monitor all company assets. Group IT monitor all components of SimCorp's infrastructure, including network drives, hard drives of computers connected to the company's network, and accessed websites as described in section 8.7. Serious cases of non-compliance will be reported to Group HR, Group Legal and/or Group IT, depending on the nature and severity of the breach.

SimCorp reserves its right to disclose all information, including text and images, for the purposes of law enforcement without prior consent of the sender or receiver.

13.4. Employee violations

Any breach by employees of this Policy may lead to disciplinary sanctions, in accordance with SimCorp's general policies and Employee Handbook This includes an oral reprimand, a written warning and/or termination of employment depending upon the type and severity of the violations, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

14. How to report Information Security Issues

Security issues should be reported with no delay.

Group IT Service Desk can be reached 24/7/365 on phone + 45 3544 **8998**

Any questions regarding this Information security policy should be raised to:

Information Security team, alternately IT management

Change log

Version 1.0 (October 2013): KAL: Revised wording of several sections, changed policy for user installation of software

Version 1.01 (December 2013): Minor revisions

Version 2.0 (October 2014): KAL: Incorporated changes based on EMB and Board of Directors review. Procedure text edited or removed. No major changes to actual policies.

Version 3.0 (September 2015): KAL: Made additions to clarify position on cloud services and network anonymization tools. Included wording about awareness training and testing.

Version 3.1 (October 2016): KAL: Annual review performed, no changes.

Version 4.0 (October 2017): KAL: Annual review, clarifications related to private use and monitoring.

Version 4.1 (October 2018): KAL: Annual review, minor wording clarifications

Version 4.2 (May 2020): KAL: Annual review, minor clarifications

Version 4.3 (May 2021): KAL: Annual review, and mapping to ISO27001 for completeness. Some wording clarifications, and a decision to create a separate Encryption Policy and Information Classification Policy to supplement this policy.

Version 4.4 (May 2022): KAL: Wording clarifications, minor additions, and merge with SCDaaS Security Policy