DOCUMENT ID	AUTHOR Jonas Lilja
DOCUMENT TYPE Steering Document	PROCESS Management
REVISED DATE / BY 2022-04-21 / Fredrik Sandin	APPROVED DATE / BY 2022-04-21 / Lars Kry

INFORMATION SECURITY POLICY

Nexer Group AB (referred to hereafter as ”Nexer”, ”we”, or ”the company”) and the Nexer group’s vision is to create a better tomorrow for our customers, our employees, and for the world around us. With this in mind, we will always protect our customers and our internal information against loss, distortion, and unwanted access by unauthorized entities. We do this through technical IT security protection as well as employee knowledge and awareness of the threats against information security. These protective measures also ensure that our business has easy access to information as well as efficient information handling, with a traceability that supports our business.

Information security policy protective measures must fulfill customer-specific requirements in agreements, legal requirements, and supplier agreements, as well as the general requirements that are documented in this policy. Our information security must also serve as a trustworthy sales argument for our services.

This document describes the rules for usage of ”IT resources” within Nexer, and is based upon a regulatory framework, which is a general standard across Nexer. The term ”IT resources” includes computers, tablets, telephones, networks, systems, cloud services, and other equipment that is used in handling information in digital form.

All personnel as well as any other users of Nexer resources are obliged to follow this information security policy.

POLICY CONSTRUCTION AND GENERAL

This document is divided into an introductory general information section containing general rules, as well as an appendix, which describes in more detail certain aspects of company and system-specific terms.

We will continually work to improve information security and compliance in order to raise the objectives from year to year.

We are a learning organization that will keep ourselves updated on technical development in the areas of IT security and data protection. Education in information security must be completed by new employees and repeated every second year. This is the joint responsibility of the co-worker and management.

GENERAL RULES

Company (and Nexer Group) IT resources must not be used to improperly spread, store, or convey information:

- which is contrary to current legislation, for example, baiting certain ethnic, religious, gender-related groups; child pornography offences, unlawful depiction of violence, slander, abuse, hacking, or copyright infringements
- which is regarded as political, ideological, or religious propaganda
- which are in violation of GDPR provisions on personal integrity
- which can be otherwise interpreted as slanderous and offensive
- which has the purpose of marketing products or services that are not affiliated to the company
- that in any other way can interfere with company IT operations.

Penalties for Violation

Company employees or other affected parties who in any way violate this information security policy are personally responsible for the infringement committed. The nature of the infringement will determine the penalties. Penalties can include a verbal or written warning, and in serious cases the violation may result in termination of employment from the company. Users that are suspected of criminal activity may be reported to the police.

STORAGE OF INFORMATION/DOCUMENTATION

Information should be stored primarily in our IT environment according to the chart below, and never only on a local hard drive. Employees are responsible for ensuring that information is not lost due to computer problems.

Documentation / Content	OneDrive	MS Teams	Intranet	Agda or Catalyst	Cinode	Lime	IM/ DCE	Other*
My Personal files	X							
Project/service teams		X						
Org teams/units		X						
Common internal information			X					
Employee's personal information				X				
CVs					X			
Client framework agreements						X		
Client assignment agreements						X		
DPA						X		X
Purchase agreements							X	
Source code, CAD, VM, Large data volumes								X

* For example, fileserver, NAS, and other storage services that fulfill the requirements below.

The use of extra cloud services can sometimes be motivated by collaboration with an external party. The criteria for choosing the service is based on the relevance of the case documentation, and must take the following into consideration:

- Authentication
- Routines for deleting information
- Backup and retrieval of information
- Logging
- Intrusion protection (physical and logical).

Nexer E-mail addresses should be used as user accounts. If the external party administrates the service, then copies of commercially important information should also be saved to our internal IT environment.

If non-public documents or media are stored externally (for example, on a hard drive or flash storage stick), the documents and/or media must be encrypted and deleted when they are discontinued.

PERSONAL INFORMATION

Handling of personal data requires special care. All co-workers who have access to personal data, internally or for external customers, must be familiar with the requirements of the EU regulations in the area, GDPR, and follow the company policy for protection of personal data. For handling personal information of customers, especially where it includes sensitive information, each individual employee who is involved in such processing is responsible for ensuring that he/she has access to all instructions regarding handling of such information (even if it is the responsibility of the manager to instruct the employee on which instructions are relevant).

IDENTITY AND PASSWORD POLICY

Employees are responsible for protecting the authentication process for the information systems and storage functions. Account information and passwords are confidential, personal, and shall not be shared or recorded on unencrypted media.

- Employees must not use the same password that is used to access company resources for external systems or private use (for example, Facebook or Gmail).
- Passwords must be at least 8 characters long and must contain at least three of the following: a number (0-9), a capital letter (A-Z), a lower-case letter (a-z), or a special character.
- The passwordd should not contain portions of your name or account name.
- The password should not contain portions of the company name.
- The password should be changed at least 2 times yearly (forced update).
- Multi factor authentication such as authenticators must be used wherever possible. These rules are enforced internally, but employees should strive to follow them when creating accounts or selecting credentials for external services used in connection to work or company information as well.

PHYSICAL PROTECTION OF THE PREMISES

Our offices must be protected according to the latest approved directives to the office managers. All employees are responsible for following the office rules regarding entry/exit to the facility, escorting visitors, fire safety and alarm procedures, locks and surveillance. For our four largest offices (Göteborg, Stockholm, Malmö & Örebro), the protection class must be 2. For all other offices its recommended to have 2 but local decisions can be made if accepted by office responsible, responsible business area manager and security manager.

WORK AT OUR OFFICE

Information management when working at the office should be handled with regard to the relevant information security class. Customer information must be kept restricted within a defined user group. This policy follows the commercial terms that Nexer is bound by, where it is stipulated that customer information (which usually is protected by confidentiality policy) should only be shared with those employees that need access to it in order to perform relevant work. Printed information cannot be left unattended on desks or at the print station. Password-protected screen savers should be used when computers

are left unattended. Unidentified persons who are found in the office must be approached and escorted to their goal or to the nearest exit.

Clean Desk Policy: Laptop computers must not be left at the workstations at the end of the day, except in special circumstances and only if specific security precautions are taken.

It is not allowed to connect personal network equipment, including routers and access points, unless there is a special circumstance and specific security precautions are taken. All network equipment must be delivered and configured by Nexer's network service provider. Exceptions must be approved by the company's security protection manager and/or the CEO.

DISTANCE WORK

Working outside of the office requires special vigilance in any environment where unknown persons are present. Equipment and documents should not be left unattended or in a locked vehicle. Verbal conversations about work/customers must be conducted in such a way that eavesdropping by unauthorized persons is not possible. Monitor shield screens must be used so that unauthorized persons cannot see the display.

While working outside the office, employees should avoid using public wireless networks or public USB ports for charging, such as those that can be found in airports, trains or shopping centers. If a public network must be used, care should be taken to safeguard any sensitive information sent, and employees should assume that digital eavesdropping is taking place.
Whenever possible, distance work should be conducted using a VPN connection

ACCEPTABLE USE OF RESOURCES

Employees are allowed to bring their personal laptop with them when leaving the office, as well as any documents they require to accomplish their assignments. Any resources brought outside the office must not be left unsupervised or in a locked vehicle.
In certain cases where the laptop and/or documents have a heightened need for protection a manager's approval is required. Handling of the resources must adhere to the information classification policy, and any protective measures prescribed therein must be taken.
Employees should avoid handling (reading, storing, writing, sending etc.) company information, files or messages on private devices such as their own computers or smartphones, private email accounts or private cloud storage accounts, and should instead prefer to use the resources provided by or connected to Nexer.

EXTERNAL COMMUNICATION

Communication with external parties must be conducted so that the security requirements for all involved are met. Customer requirements on information security must be clarified and communicated to everyone involved. Employees are individually responsible for fully understanding which privacy terms and regulations are applicable for the sharing of

confidential and/or sensitive external communication. Breaches of the confidentiality agreement could result in Nexer being held liable for damages.

An agreement can be made with external parties regarding password-protected documents or encrypted E-mail messages. Data communication musttake place with the support of technical protection which is kept updated.

No confidential business information may be sent or automatically forwarded to private E-mail accounts.

Private use of E-mail is allowed, but must follow our information security policy. Employees accept that messages are logged in the same way as all other E-mail traffic. E-mail can be opened and read by staff other than the addressee if the situation is called for. Nexer E-mail addresses may not be used for private registration of e-services.

PROTECTION OF COMPUTER EQUIPMENT

Mobile telephones and tablets shall always be protected with code lock. In the event of settlement, company information such as E-mail account must be deleted.

All company computers must be protected with passwords on the screensaver as well as encrypted hard drives if confidential data is stored there.

In the event of termination of employment and with new equipment acquisition (exchange), the old computer must be submitted to their manager. The manager is responsible for data routing as well as delisting from the inventory register, “Nexer Active Directory”. Licensed software with significant value (>3000 SEK) is returned to the company.

HARDWARE

Computers, monitors, network equipment, and printer/copiers are managed centrally, with established routines for purchasing, exchange, and liquidation. Periferal equipment and accessories may, with exception, be purchased outside of the central function if it facilitates the assignment and customer delivery. Computer and network equipment that is purchased locally may not be connected to the company's Active Directory or internal networks. Customer hardware that is used in the assignment shall be handled according to the agreement.

In the event of loss or damage to company IT resources, the security manger should be notified at once, who in turn reports to the Service Desk for instructions on appropriate action.

OPERATING SYSTEM

The Microsoft® platform(s) is the one we primarily use to build our common system support and compatability for. We have limited central support for OSX. Other platforms such as Linux and Google Chrome are accepted as assignment-specific exceptions and are not covered by our general functional and accessibility measures. Support for these exceptions is limited. They are allowed to be used in our system and network in such a way that does not affect the overall infrastructure. The responsibility for licensing, support, competence, and compatibility for other platforms than Microsoft and OSX rests with the manager of the unit that uses those platforms.

PROTECTION AGAINST HARMFUL CODE

Company computers must have centrally-maintained protection against harmful code, and employees are responsible for ensuring that centrally-distributed updates are installed on their computer. Employees are responsible for maintaining vigilance against the more and more sophisticated intrusion attempts via E-mail, telephone calls, and other means. It is not allowed to deactivate the virus protection program and/or firewall without the company security manager's approval.

Program installation on the computer must be motivated by work usage. Programs for private use are generally not installed on Nexer computers.

External computers on company premises may only be connected to the guest network, for example the guest Wi-Fi. Any software with potential offensive capabilities such as vulnerability scanners, pass-word crackers or other forms of utility software designed to circumvent, assess or break security measures may not be utilized by employees unless it is required by their assign-ment or can be motivated by their role or responsibilities.

USAGE OF THE INTERNET AND SOCIAL MEDIA

It is not allowed use company computers to visit websites that are used for illegal activity or which can cause offence. All usage, including information on visited sites, is logged. Using copyrighted matieral/photographs may only occur with proper permissions. Private communication via social media within professional subject areas is encouraged.

INCIDENTS AND VULNERABILITY

All employees are responsible for reporting suspected or detected incidents and vulnerabilities concerning personal data, IT security, or our physical security. This is done via the form on the Intranet, clicking the button “Report Security Incident”.

IT security incidents and vulnerabilities of an urgent nature should be reported immediately to the Service Desk. Suspicious activity or discoveries that do not require immediate action can be reported via the form on the Intranet, clicking the button “Report Security Incident”.

Examples of technical incidents: computer infected by virus or malware, an email containing sensitive information sent to the wrong recipient, someone else gaining access to one or more of your accounts, theft or loss of sensitive information or personal information being handled in a bad or unsecure manner.
Examples of non-technical incidents that should also be reported: someone you do not recognize follow you through an otherwise locked door, unknown person contacting you asking for information, break-in, someone trying to look over your shoulder or eavesdropping when you’re working, theft or loss of a computer, storage device or phone containing or previously have contained company files, messages or information

APPENDIX – NEXER GROUP

Nexer AB
Nexer Enterprise AB
Nexer Insight AB
Nexer Recruit AB
Nexer Cybersecurity AB
Nexer Tech Talent AB
Nexer Infrastructure AB

IEC/ISO27001

ORGANIZATION FOR INFORMATION SECURITY

The overall responsibility for information security is delegated to the security manager, CIO, who in that capacity has the authority to give directives towards achieving our information security goals. The responsibility for the management system and revisions rests upon the manager for IT and process.

All personnel are responsible for following the information security policy that is associated with their role responsibility, authority, and work assignment, which is documented in each respective roll description. The confidentiality statement is signed at the time of employment and applies during and after employment. All personnel are required to comply with this information security policy.

All information that is handled has an identified information owner. The information owner is reponsible for ensuring information security through the requirements that are set on system owners and system managers, as well as on the infrastructure.

An important prerequisite for information security is that the responsibility and rolls are assigned so that incompatible areas of responsibility are not assigned to the same individual. Control and approval should not be combined with initiation and implementation.

PROCESSES FOR INFORMATION SECURITY

The information security aspect should be included in our work processes so that the risks are assessed and handled in the way that the situation requires. Assessments of threats, risk analysis, and risk management regarding information security shall be made via changes to processes and organization, and shall follow the routine that is decided upon for risk analysis

INFORMATION CLASSES

Information that is handled shall be analyzed and classified. Our internal information assets are classified based upon sensitivity/weight – legal, commercial and/or operational.

The customer information that is handled in an assignment must be classified based upon customer requirements. These should be discussed in depth before the contract agreement is signed, so that the customer documentation is handled with the correct information class and so that the assignment is otherwise based on the correct information security requirements.

The information class controls the permissions for our information system and how information/documentation should be handled. See the model below.

Information class	Brief description based on the criteria above
Internal	Internally used information. Should be handled so that the customer and customer relationship are protected against damage. Can be shared internally but externally only with the approval of the information owner.
Confidential	Information that is considered sensitive/important for legal, business, and/or operational reasons. Should be accessible only to people who need it for their duties.
Secret	Information that is judged extemely sensitive for legal, busines and/or operational reasons. Access is managed by the information owner himself.
Public	Information that has been completed for external communication. Should be protected against unauthorized modification and can then be freely distributed.

All employees must have knowledge on our information classes and on how to handle information according to the regulations for each information class. See further documents: (in Swedish) Information Classification – Model and implementation.

IT SECURITY PROTECTION

Employees who work with operations, support, development, and maintence in customer assignments or internal systems are required to comply with the IT security policy, which is more technically oriented.