digitalmind

NDB-PO-0005

INFORMATION SECURITY POLICY

Purpose	Define clear and understandable Information security policy, information security focus and goals, and association with Information Security Management System.
Managerial responsibility	Each manager bears responsibility to ensure that this normative document is known and conformed to by all employees within his/her respective area of responsibility which at some stage might be involved in activities relating to this normative document, and to act in a manner that sets a proper example.
	All Company employees, as well as to all subcontractors and suppliers who have access to Company information sources.
Applies to	All group companies

Target audience	Process group	Document date	Document version	Review date
All company	Compliance	04.12.2024	4.0	30.11.2027

Table of contents

INFORMATION SECURITY POLICY

OVERVIEW

Main objectives of information security policy are to preserve confidentiality, integrity and availability of systems and information used by organization.

Management periodically (at least once a year) reviews, evaluates, and adjusts information security policy objectives and oversees their implementation. Policy is reviewed additionally if there is increased human caused incident count (over 10).

Management is committed to satisfy with applicable requirements related to information security.

Our Information Security policy focuses on the following aspects:

Confidentiality: protecting sensitive information that is entrusted to us by our clients or used internally as nonpublic information containing personal information, confidential data, or any other sensitive data.

- Control access to information and prevent unauthorized access.
- Prevent data breaches and leakages.

Integrity: data accuracy and quality to ensure no harm to data owners and organization.

- Mitigate human error risks, Ensure trackability.
- Prevent malicious actors from gaining access and changing information.
- Establish change control process.

Availability: information accuracy, consistency, and completeness to ensure the right information is accessible to users in the right place and time.

- Prevent impact from disasters and human error.
- Maintain data and establish processes and rules to maintain data integrity.

SUMMARY

The policy defines:

- General information security standards for Company information systems, related infrastructure and the information stored and processed by them
- Unified approach, configuration, and behavior, ensuring high degree of information systems security
- Responsibilities regarding information security throughout all group companies

The policy is intended to help make the best use of the IT resources at our disposal, while minimizing the security risks. As an individual reading this, you should understand the following:

- You are individually responsible for protecting the equipment, software, and information in your hands. Security is a joint responsibility;
- Identify which data is non-public, which includes company confidential data, client data and personal data as further described below. If you do not know or are not sure, ask. Information is an asset, sometimes a priceless asset;
- Use the resources at your disposal only for the benefit of the Company;
- Understand that you are accountable for what you do on your system;
- Protect equipment from loss & theft. Only store data on encrypted devices;
- Do not bypass established network and internet access connection rules;
- Do not bypass or uninstall your virus checking or firewall software;
- No piracy using company's devices or network, do not process, download any information or data that is protected by privacy laws and Company has not obtained the right to use it;
- Do not change or install any unauthorized software;
- Do not copy or store Company data on external devices or unauthorized external locations which are not company approved services. Contact Internal Support for the best solution for secured file transfer when this is required;
- If you become aware of a potential or actual security incident, you must report the incident as soon as possible by contacting Internal Support.

The policies and supporting standards must be read, understood, acknowledged, and followed by all Company staff including employees of related companies.

ASSET MANAGEMENT POLICY

ASSET INVENTORY

Company group uses a variety of information assets, ranging from laptops, servers to software (both in cloud and on-prem). An inventory of these assets and software assets needs to constantly be maintained and must include the following details for all significant information assets belonging to, or used by the company:

- Asset name and characteristics
- The information/data owner
- The custodian of the information
- The sensitivity of the asset, due to regulations, customer expectations, laws or other requirements
- Requirement for the asset regarding availability, uptime, business continuity, etc.
- Lifecycle information (e.g., next review date / reallocation date / start and end date)

Full list of information management systems should be part of asset inventory to support proper information governance.

HARDWARE MANAGEMENT

Hardware lifecycle approach to hardware management:

- Hardware must only be acquired from approved vendors
- Only approved software configuration should be applied to new hardware
- End-users should take appropriate care with any hardware that has been issued to them
- Lost/Stolen hardware must be reported immediately to Internal Support
- End-of-life hardware should be securely disposed

INFORMATION ASSET DESTRUCTION

Destruction of all information assets, including physical documents, electronic data, storage devices, and any other form on information shall be carried out when information assets are no longer needed or have reached the end of their retention period.

Asset owner is responsible for ensuring that information is destroyed in compliance with company's policies. Internal IT can provide support in the secure destruction of electronic data and media.

Destruction of information assets should be carried out according to type of asset:

- Data sanitization (electronic data): ensure that storage devices and media are sanitized, when possible, use software that overwrites data multiple times and destroy the media physically if sanitization is not possible.
- Destruction of physical documents: Sensitive or confidential documents should be shredded to render information unreadable, in case or large volumes of physical documents – certified third-party vendor who can provide a certificate of destruction should be used.
- Destruction of other media: use appropriate method to the type of media, such as shredding or crushing.

Records of destruction should be maintained and information assets periodically reviewed.

INFORMATION MANAGEMENT POLICY

INFORMATION CLASIFICATION

Information security policy focuses on the protection, or 3 components of information stored on Company systems: **Confidentiality**, **integrity** and **availability** whilst ensuring data privacy.

All information must be classified based on these 3 components to allow implementation of the appropriate levels of protection in line with its criticality and to ensure that the controls applied to it are sufficient and do not impair the company's business. Information classifications are detailed in the information classification matrix.

Type	Usage	Description	example
Public	No restrictions	Any business data that is easily accessible by the public and cannot cause any significant damage to company. This information can be shared with any individual or organization.	Blog entries, information on DM web site, press releases, publicly distributed information
Internal use *(default for any unclassified information)*	For internal use only without restrictions, may be copied as necessary.	Information that can be used and shared within the company. This information doesn't contain any customer or partner sensitive information and it cannot leave the company.	Policy, guidelines, internal emails, project guidelines, best practices and accumulated know how on specific products and/or technologies
Confidential	Use internally. Share with employees in the same authorized group. Can be copied if necessary. Store in an appropriate safe place.	Information classified as confidential contains sensitive customer, partner or employee information. This information may leave company for sharing with appropriate customer or partners. All partner, customer and employee data is considered confidential by nature.	Customer information, contracts, proposals, analytical documents, conceptual documents

Restricted	Unauthorized distribution prohibited. Copies are numbered and registered.	This is highest sensitivity. Information classified as restricted contains highly sensitive company internal information. This information cannot leave company and must be used, processed and shared only by identified persons. Disclosure of such information may lead to permanent damage.	Intellectual property, DM strategic plans, Management and shareholder documents, financial reports, budget plans and trade secrets, passwords, keys, access data.
Secret	Unauthorized distribution prohibited. Copies shall be numbered and recorded.	Classification used for government "Secret" customers.	Passwords, keys, access data, and government information are "Secret"

In addition, the client can propose a classification of his information sources, which would be subject to rational restrictions.

All company employees sign confidentiality agreement.

INFORMATION HANDLING

Information, in electronic and physical formats, should be handled in accordance with the sensitivity, risk and classification of the information:

- Ensure confidentiality agreements are in place before sharing data externally.
- When emailing sensitive files externally the files should be password protected.
- Check email addresses prior to sending any files.
- Use restricted access systems whenever possible and avoid storing sensitive information for prolonged time directly on laptop or other hardware that is used on daily bases.
- Volumes of computers used by Company should be encrypted.
- General use of external storage drives is prohibited, and files should not be copied to removable storages. In rare cases when this is needed, use of specific storage device must be approved by IT support and data should be encrypted. After data is not needed removable drive must be provided to IT support team and they will use data sanitization/wiping software to completely erase all data. Removable drives are transferred only from hand-

to-hand; no external couriers are used. Logs should be maintained by IT support of removable device usage and disposal activities; the content of the media should be established.

INFORMATION GOVERNANCE

Company uses multiple systems for storage of restricted information and data. Each of these systems has its own specific purpose and principles for appropriate use. No less than these systems should be implemented in the company for appropriate information governance:

Type	Description
Collaboration and communication tool	Used as main communication channel between company employees and for collaboration during ongoing projects. The goal of communication and collaboration tool is to provide common platform for such activities and to store as much as possible of this communication as business records.
Helpdesk / Project Management	Used for time tracking and project task administration. Also used for collaboration with customers between Company employees during implementation, SLA and internal projects. The goal of Helpdesk / Project management system is to provide customers and Company employees with efficient channel for incident reporting, task status updates and time tracking/reporting.
ECM	Enterprise Content Management system used for storage and circulation of internal documents. The goal of ECM system is to provide secure and compliant storage for business-critical documents.
ERP	Enterprise Resource Planning system used to manage day-to-day business activities such as accounting.
CRM	Customer Relations Management used for client and sales process related data (contact information, deal registration, deal progress tracking, deal reporting). The goal of the CRM system is to track the progress of sales pipeline development and provide necessary information to the sales team for more productive deal closing and account development.

Full list of all information systems must be maintained in line with principles set in asset management policy.

All information and data should be managed in standardized systems developed for such purpose (e.g., CRM, ERP, ECM, etc.).

All data should be managed in secure and compliant "on premises" system owned by Company or in "cloud-based" solution that complies with GDPR regulation, and provider of the system should be at least ISO 27001 certified.

ACCESS CONTROL POLICY

Access to information and systems under control of the Company must be provided on a least privilege, need to know basis.

All Company laptops must be protected by password or pin code and connected to Azure Active Directory where accessible only with personalized accounts (with exception of specific administration accounts). Password less connection options (fingerprint, face recognition) are allowed.

All Company servers must be protected by password and connected to domain controller.

All Company existing information systems must have 2-factor authentication enabled if possible. 2FA (2-factor authentication) must be mandatory requirement for all new internal system implementations and must be enabled / enforced.

Type	Description
User registration	Approving and / or physically giving access right to users.
Privilege management	Clear hierarchies must be determined for each system and each hierarchy must be formally approved. Any changes to existing composition must be formally approved by Internal Support and CTO of the Company.
User management	As above, each system must have clear procedure for approval and method of granting access to that system. Procedure must exist for each system for joiners, movers, and leavers, with audit trails.

User access rights are subject to periodic reviews by Internal Support.

PASSWORD POLICY

Password policy and corresponding system configuration must be periodically aligned with industry best practices (e.g., password complexity, required change intervals).

- Users must be forced to change their passwords during the first log-on.
- Users must change password if they have reason to believe that password has been compromised.
- Password expiration must corelate to password length in favor of longer passwords with less frequent change interval.
- Password complexity must be enforced wherever possible.
- Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions.
- Passwords shall be stored in an encrypted format.
- Default account shall be disabled and/or default passwords associated with such accounts shall be changed.
- Shared accounts should be used only in very rare cases and their passwords should be changed at least once a year or in the scenarios where the user knew the password and terminated business relationships.

ACCEPTABLE USE POLICY

Company IT resources may only be used for Company business related purposes.

EMAIL USAGE POLICY

E-mail is a business communication tool which all Company employees are requested to use in a responsible, effective and lawful manner.

- Only official user email should be used for business correspondence.
- Employees are forbidden to allow other person to use their e-mail mailbox or use mailboxes of other users.
- E-mail users must ensure the confidentiality of the information sent and sender is responsible for the content and security of the information sent by e-mail.

- After receiving an unwanted e-mail message (spam), it is forbidden to reply to it or forward it. The message can be forwarded to support team as evidence of a security breach only as a picture from “print screen”. Exception - upon request of support team, message can be provided to support team for further analysis by following strict instruction for each case.
- E-mail users must comply with the requirements for secure e-mail use:
    - Beware of phishing and social engineering attempts: do not open emails received from unknown senders, assess whether the email was sent by the sender (mismatch between email address and sender, strange

INTERNET USAGE POLICY

Internet access is provided to all employees to assist in carrying out their duties. Occasional and limited personal use of the internet is permitted if such use does not:

- Interfere with work performance & productivity
- Include downloading or distribution of large files
- Have negative effect on performance of IT systems or Company network in general

It is strictly forbidden to upload Company non-public information to external file transfer or storage sites, like dropbox or google drive (with exception of specific Company approved external cloud storage sites).

PORTABLE MEDIA

The use of portable media is only permitter in exceptional circumstances. When portable media is used it should be approved by Internal support and assigned a level of protection aligned with level of risk. Company reserves the right to inspect and erase portable media that is used on its network.

REMOTE ACCESS AND COMMUNICATION POLICY

INTERNAL USERS

Frequently users will be required to access company's information systems from outside the office. For remote access to the company IT infrastructure resources only the officially supported and approved facilities by the DM IT Support department are to be used (e.g., Company issued laptop using DM VPN).

Company information systems are accessible by one of two approaches:

- Point to Site VPN
- AD Application Proxy

All information systems should have 2-factor authentication enabled if possible.

Most of systems should use AD Application Proxy approach to minimize need for VPN and to reserve VPN only to access IT infrastructure itself or use defined VPN tunnels to access client systems.

Periodic review of log files should be performed to identify usage of VPN. Access to VPN should be granted only to employees with actual need for internal resources and access to client systems that are not accessible without use of VPN.

Online communication from within company network to an external party may only use DM approved communication channels. Personal internet connections or connectivity devices are strictly prohibited.

EXTERNAL USERS

Remote access to external party (customer network) regardless of used method (direct VPN or tunnel from Company network) should be accounted and logged accordingly.

For this purpose, access registry should be set up and available to all employees.

Registry entry must be created before each connection to external network. Registry entry can be and must be update after end of session to specify details about access to external network:

- Start date, time
- End date, time
- Purpose
- Employee
- User account that was used
- Short description of task performed

SYSTEM CHANGE AND CONFIGURATION POLICY

All changes must be conducted in a controlled and approved way. Company IT support system is used for change monitoring and approval.

System changes or re-configuration is allowed only after approval of data owner of specific system/resource.

In scenarios where system changes are tied with additional expenses/new pricing plans, then data owner should consult with CFO before approving tasks to IT support.

Data owner has direct knowledge and involvement in the creation/using of the data. They will determine who has access and at what levels. Data owner should also have input into data retention and data destruction policies.

In many systems, but not all, IT support team is both the data custodian (protects data, applies controls etc.) and system owner (owns the server).

Small routine and technical changes do not need approval, but these changes are still logged.

Employees are informed about system changes that will impact them in timely manner via maintenance plans and internal communication tools (Teams, e-mail).

System baseline should be established as part of change management database to keep track of system allocated resources, software versions and other aspects.

NETWORK PROTECTION POLICY

A secure network is critical to the security of business:

- External facing networks should be firewalled to an appropriate level
- Physical and logical network changes should only be made by or under supervision of Internal Support
- Network event logging and monitoring should be implemented
- Segregation in networks should be implemented to separate various network zones.
- Third-party users shall not connect their computing devices to the wired or wireless network of Company unless authorized by Internal Support. Guest wireless can be provided and must be separated from Company corporate network. Wireless networks should always be encrypted.

EVENT LOGGING AND MONITORING

Adequate monitoring controls to detect attacks and unauthorized access to its information processing systems must be implemented. The level of monitoring required shall be determined by risk assessment and any relevant or applicable legal requirement shall be identified to ensure that the monitoring activities comply with the requirements. Monitoring of employee (both standard users account and administrator accounts) may consist of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Helpdesk tickets
- Vulnerability scanning
- Other log and error files

Regular Log file review shall be performed by Internal Support by use of automated monitoring scripts and tools where applicable.

Local logging should be enabled on all systems and network devices.

Log files and log systems are protected against tampering and unauthorized access.

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

WORKSTATION SECURITY POLICY

Workstations include laptops and desktops:

- All workstations should have corporate-approved anti-virus software installed and enabled
- All workstations should have local firewall enabled. Changes to local firewall rules must be coordinated with IT support.
- All workstations should have a password protected screensaver with short timeout period to ensure security of unattended workstation
- Only Company owned devices and configured by IT support are considered secure (for details see BYOD policy)
- Only authorized software can be installed without approval of Internal Support
- All laptops should be encrypted
- Only install software from trusted sources
- Do not allow unauthorized users to access your workstation
- Take appropriate steps to maintain the physical security of your workstation.
- All workstations should have user access control configured (UAC) which notifies and waits for user approval about system wide changes.
- Usage of utility programs like antivirus, compressions tools, file management systems is allowed for employees on daily basis.
- Usage of utility programs like network scanners and analyzers, disk partition editors, registry editors etc. is allowed only with approval of IT support.

MOBILE DEVICE SECURITY POLICY

It is prohibited to store Company internal, confidential, or restricted information on mobile devices. Employees should avoid storing any document or other Company data on mobile device. Employee is responsible for deleting any temporary or saved data from mobile device if such data is stored after accessing Company internal systems.

Access to Company information systems from mobile device is allowed only by using mobile device with configured mobile device management (MDM) solution.

REQUIREMENTS FOR MOBILE DEVICE

Device must be pin code protected with at least 6 digit code.

In the event of the loss of a mobile device or unauthorized access to a mobile device, the user should contact Internal Support and initiate security incident to mitigate risks of company non-public data exposure.

BRING YOUR OWN DEVICE POLICY

Only Company owned devices are considered trusted and can be connected directly to the Company LAN or corporate wireless network.

All other devices are by default considered as untrusted. Untrusted devices must never be connected directly to internal network, neither through a network cable nor through wireless network. Untrusted devices are only allowed to use Guest network access in Company office.

In rare exception case when device not owned by Company must be connected to Company network, device must be submitted to Internal Support for inspection, evaluation, and adequate protection measure setup (e.g., MDM, company anti-virus software, malware protection, encryption, etc.).

Unless explicitly approved by Internal Support and made “trusted”, device not owned by Company should never be used to store company non-public information.

While Company is determined to ensure security of all information, bringing your own device is an option that will be evaluated on case-by-case bases. To ensure security of Company information and enforce certain conditions and rules – BYOD agreement should be in place for each case.

Agreement should define clear rules for onboarding and offboarding such device:

- Procedure for reporting lost or stolen device
- Requirements for anti-malware software
- Requirement to submit device for data wipe during offboarding

SOFTWARE DEVELOPMENT AND MAINTENANCE POLICY

Main purpose of the policy is to ensure that information security is integral part of information system across the entire lifecycle. Policy is used to ensure that development environments are secure and that processes for developing and implementing systems and system changes encourage use of secure coding and development practices.

Company acquires software only from trusted partners and ensures that software is supported by vendor and appropriately handled according to vendor recommendations.

Own development for internal use ensures testing is performed before any changes are made to production systems and security requirement are defined as part of development.

Company also provides system implementation as a service. Systems used in service delivery are from trusted long-term partners who develop their products strictly using secure coding practices and security by design approach. These are out of the box products with built in tools for customization and malicious attack risks mitigation. Customization of the product is done with tools provided by vendor and/or additional custom scripts or functionality is added inside system objects built for that purpose. Vendors are providing guides for system security proofing and guidelines for customizations to avoid risks of vulnerabilities. All development is performed in line with best practices and recommendations of OWASP to avoid OWASP top 10 vulnerabilities. Regardless of the used product, each implementation is undergoing the same phases – definition of requirements, planning and design, implementation, testing and maintenance.

Customizations have rules and boundaries set by vendor and do not increase overall security risks of the system. In case complete custom development is needed for integrations or other services outside of system boundaries – security requirements are defined together with customer during regular requirement gathering. Planning and design of customization is done with focus on set security requirements.

INTERNAL SOFTWARE DEVELOPMENT, DEPLOYMENT AND MAINTENANCE

- Application should be thoroughly tested in test environment before they are submitted to Internal Support for approval and transfer to production environment.
- Security requirements for software should be determined, documented as part of development process.

- Software changes must be approved by CTO of the company.
- Only authorized users are permitted to deploy software changes.

This applies only to software Company is maintaining and developing for internal use. E.g., ECM system add-ons and configuration, Helpdesk configuration and plug-ins etc.

LICENSING POLICY

LICENSING POLICY

Company uses software from a variety of third parties, copyrighted by the software developer and, unless expressly authorized to do so, employees do not have the right to make copies of the software.

Company policy is to respect all computer software licenses to which Company is a party. Also, Company policy is to manage its software assets and to ensure that Company installs and uses only legal software on its workstations and servers.

SOFTWARE CONTROL

As part of software asset management, Company maintains list of all software that employees are authorized to use for any business purpose.

Software used by Company employees should be supported by software vendor and receiving software update to ensure security and integrity of used software.

Use of only approved and authorized software should be ensured by regular scans of devices connected to Company network.

ENCRYPTION POLICY

Encryption is required to be used to protect company non-public information from being disclosed to unauthorized parties. Full volume encryption must be enabled on all workstations. Internal Support will perform periodic review of all workstations to ensure appropriate encryption settings are used.

All personnel are responsible for assessing the confidentiality level of data sent or residing on the devices they use. If data is non-public, all employees are responsible to comply with the encryption policy.

All web interfaces for information systems should be protected with HTTPS protocol and latest TLS version encryption should be used over SSL encryption versions where technically applicable.

BACKUP POLICY

Company Backup and restore policy provides a framework for ensuring that Company information in scope of this policy will not be lost during an incident affecting availability or integrity. Similarly, all media containing backups or Company data must be protected according to the classification related to data confidentiality, integrity, and availability, whilst ensuring data privacy.

Both data classification and backup requirement must be determined by the asset/data owners and communicated to Internal Support for implementation. Asset/data owners are responsible to inform Internal Support in writing of the specific backup requirements for each asset and of the required backup retention period.

MALWARE PROTECTION POLICY

A process must be maintained to ensure that malicious software cannot enter the Company's secure IT environment. This includes regular anti-malware update, scheduled malware scans and monitoring of events and incidents related to malware.

All company laptops or other workstations used in company network or accessing client network must have anti-malware software installed. Anti-malware software engine and databases are updated on regular basis. Presence of anti-malware software should be checked on regular basis by automated tools to ensure security of IT environment.

Microsoft Defender for Office 365 Plan1 is implemented. This configuration scans all attachments and links in SharePoint, OneDrive, MS teams, e-mail.

General use of removable storage devices is prohibited, all devices should be configured to:

- Automatically scan any connected removable media for malware
- Not auto run any content from removable devices

SECURITY INCIDENT MANAGEMENT POLICY

Security incident management policy details the framework for early detection, reporting and responding to security incidents. Information security incidents and failures are registered based on Incident Management procedure and identified in incident reporting system.

All security incidents whether actual or suspected, must be reported as soon as possible by one of the following methods:

- Escalation by telephone to member of the Internal Support. Particularly if the personnel consider the incident to be of high risk, or
- Notification to the Helpdesk / email to Internal Support.

Even if a Security Incident is not considered to be serious, it should always be reported as it may be part of a wider issue or trend. Additionally, first appearances of the severity of the Security Incident may be deceptive and not indicative of the severity of the underlaying risk.

After incident has been contained and affected systems are returned to normal operational status, incidents must be documented and thoroughly investigated to detect cause, calculate impact and prepare strategy to prevent similar incidents in the future.

The Information Security Officer evaluates information security incidents at least once a year.

The information Security Officer initiates the annual information security risk assessment.

The information Security Officer performs the risk assessment or delegates this task to team of employees.

BUSINESS CONTINUITY MANAGEMENT POLICY

Company should maintain a group Business Continuity Management Policy. This requires sub-functions to develop detailed business continuity plans under its umbrella. The IT function must ensure that the Business Continuity Plan (BCP) adequately addresses business continuity of the Company's IT environment.

DISASTER RECOVERY PLANNING (DRP)

Disaster Recovery Planning is a subset of BCP. Given the importance of this aspect of the BCP, the key attributes of a disaster recovery plan are discussed below. There are various categories of disruptive events covered by our BCP/DRP:

- Loss of data, which may include loss or program and system files
- Unavailability of computer and network equipment
- Environmental disasters
- Organized/deliberate disruption
- Loss of utilities/services
- Equipment/System failure
- Pandemics
- Cyber Attacks
- Other (health and safety, legal, etc.).

Recovery requirements must be determined by the asset owner based on the criticality of the processes of the Business Functions that use the IT systems (determined through Business Impact Analysis). The asset owner will ensure the following:

- Sufficient documentation of each Disaster Recovery plan, needed to enable efficient execution of the plans
- Disaster Recovery Plan which specifies the appropriate security measures to ensure the degree of confidentiality and integrity required for the recoverable systems
- That the Disaster Recovery Plan specifies a regular procedure for making copies of data from which to recreate originals in case of a disaster. Disaster backups should not be used for operational recovery
- The Disaster Recovery Plan must be tested on a periodic basis

PHYSICAL SECURITY POLICY

Company group offices on daily basis are used by Company local employees or visiting employees from other countries / group companies. There are also clients who are visiting Company office, potential clients, office building administration, outsourced IT partners and occasional contractors for specific tasks. Besides main office, work from remote locations (e.g., customer site, employee's place of residence) is allowed.

The purpose of this policy is to provide a framework and procedures for identifying and dealing with security risks. Policy describes reasonable practices to ensure the safety of Company assets.

Policy:

- Defines rules and responsibilities of relevant persons
- Confirms Company commitment to ensure safety of all assets
- Defines practices and rules at Company office
- Defines practices and rules that should be used at remote locations to minimize security related risks
- Defines rules and control measures when dealing with any visitors

OFFICE – GENERAL SAFETY

Every Company employee must ensure that no important information asset shall be left on desks unattended, especially during non-work hours.

Company security is dependent on the physical security of our resources at on-premises computer room/data center.

- All entry points to Company IT facilities should be locked and key available only to specific approved persons
- Appropriate environmental controls such as air conditioning and fire suppression system should be in place
- There must be at least battery backup power onsite with sufficient duration to safely shut down all systems in case of power loss
- Visitor access should be controlled

OFFICE – ACCESS CONTROL

Every Company employee has electronic access card to access Company facilities. Access cards should not be exchanged between employees or trusted to third party. In case of access card loss, it must be immediately reported to office building security or Internal Support. All issued access cards should be accounted and listed in Company asset inventory.

REMOTE LOCATIONS

Every Company employee must ensure safety of Company assets while working from remote location. Workstation (e.g., laptop) or any other asset should not be left unattended at any publicly accessible location.

- **Virtual Private Network (VPN)** should be used in all cases when access to Company network is required. VPN should be available only to employees with actual need and permission to access Company internal IT infrastructure resources or client systems that are not accessible without VPN. Access to most Company information systems should be provided via Active Directory application proxy approach without need to use VPN.
- **Wi-Fi connection**. WIFI connections at public places like shops, restaurants, airports and similar should never be used as these are primary spots for malicious parties to spy on internet traffic and collect confidential information. Personal mobile hotspot can be used as a safer alternative to public Wi-Fi.
- **Home routers**. Default passwords must be changed to prevent access to traffic and employee should take appropriate additional steps to ensure security of his network infrastructure (e.g., update firmware on regular bases).
- **Two factor authentication** should be used to access Company information systems.

COMMUTING

Every Company employee must ensure safety of Company assets while transferring to and from remote location. Employees should never leave any assets in visible places (e.g., interior of parked car).

CONTROLLED VISITOR ACCESS

- **All visitors** without access to office entrance should check-in at building security or front desk and should be cleared by Company employee for office access. Exception is building administration or building administration contractors who have general access to office building.
- **Any visitor** must be met by Company employee for actual access to Company office and must be escorted when leaving.
- Visitors like clients, partners and potential clients should have only limited and supervised access to facilities where employee work desks are located to minimize risks of unintentional access to sensitive information (e.g., call with another client, employee working on another client's systems, etc.). If possible, all meetings should take place in meeting rooms.
- Visitors like contractors or building administration should be met and supervised by Company Internal Support or Head of Administrative department.

DISCIPLINARY POLICY

This Disciplinary Policy is established to enforce compliance with the company's Information Security Management System (ISMS) as per ISO 27001 standards. Its aim is to ensure that all employees adhere to the established information security protocols and procedures, thereby safeguarding the organization's data and information assets.

Company is committed to maintaining the highest level of information security. Any actions that compromise the confidentiality, integrity, or availability of the organization's information assets are subject to disciplinary action, up to and including termination of employment or contracts.

RULES AND VIOLATIONS

The following actions constitute violations of the information security policy:

- Unauthorized access to confidential data.
- Disclosure of sensitive information without proper authorization.
- Tampering with or disabling security measures.
- Non-compliance with established information security procedures
- Misuse of assigned assess privileges.

REPORTING AND INVESTIGATION

Reporting: Any suspected security breaches must be reported immediately to the Information Security Officer (ISO) or designated authority.

Initial Assessment: The ISO will conduct an initial assessment to determine if a full investigation is warranted.

Investigation: A formal investigation will be conducted, ensuring confidentiality and impartiality.

DISCIPLINARY ACTIONS

First Offense: Formal written warning and mandatory security training.

Repeat Offense: Suspension without pay, pending further investigation.

Serious Breach: Termination of employment or contract, legal action may be considered.

APPEALS

Employees may appeal disciplinary decisions by submitting a written request to the Human Resources Department within ten working days of the action.

RECORD-KEEPING

Detailed records of all security breaches, investigations, and disciplinary actions will be maintained for auditing purposes.

CHANGE REGISTRY

Date	Version	Description of changes	Approvals
11.10.2021	1.0	• Document created	Rinalds Sluckis Edgars Alksnis Aivars Baļčūns
28.11.2022	2.0	• Document transferred to new template • Policy updated in accordance with findings of internal ISO/IEC 27001:2013 audit report	Rinalds Sluckis Edgars Alksnis Aivars Baļčūns
11.12.2023	3.0	• Policy updated in accordance with findings of internal ISO/IEC 27001:2013 audit report	Rinalds Sluckis Edgars Alksnis Aivars Baļčūns
04.12.2024	4.0	• Policy updated in accordance with internal ISO/IEC 27001:2022 audit report	Rinalds Sluckis Edgars Alksnis Aivars Baļčūns