INFORMATION SECURITY POLICY - EXTERNAL

NDD TECH LTDA

Guidelines

These are the basic principles that govern NDD Tech's Security Policy, established according to the company's needs:

1. NDD is entrusted with safeguarding information from its direct and indirect clients, suppliers, and employees. Therefore, creating an environment that ensures availability and protection is essential for the Company's business continuity.

2. All information must be formally classified regarding its confidentiality, integrity, and availability, regardless of its storage form, digital or otherwise.

3. Personal data and information related to identified or identifiable natural persons must be protected in accordance with the General Data Protection Law (LGPD) and treated as confidential when there is no legitimate justification to the contrary.

4. Extra care must be taken regarding Sensitive Personal Data, those that may reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic or biometric data, health-related data, or sexual orientation.

5. Information must have a scheduled lifecycle. Information considered confidential, when no longer needed, should be destroyed through appropriate mechanisms. The disposal or reuse of media containing such information must be done in a way that renders its recovery unfeasible.

6. Every individual who has access to NDD premises must be identified. Third-party access to areas where physical or digital information processing occurs must be based on strict necessity and always occur under the supervision of an NDD employee responsible for the information in that area.

7. All equipment in the Company must be inventoried and individually identified.

8. Access credentials, or access badges to facilities and/or systems, are personal, not shareable, and non-transferable. The user is responsible for all activities carried out through authentication with their credential, therefore they must ensure its protection and confidentiality, and perform appropriate maintenance actions for each type of credential, such as periodic password changes.

9. NDD employees, during and after the termination of their employment or service contract, cannot appropriate information or media, equipment, components, or accessories containing them, such as corporate emails, spreadsheets, data files, or videos.
10. The responsibility for maintaining security is shared by all employees. NDD shall provide training to promote awareness and preparedness. Violations of the norms below, incidents, or security breaches must be reported immediately to NDD's Information Security team.

11. If there is a mere possibility of Personal Data leakage, the Data Processing Officer (DPO) must also be notified immediately.fundamentado pela estrita necessidade e deverá ocorrer sempre com o acompanhamento de funcionário da NDD, responsável pelas informações naquele setor.

Physical Security

1. Every individual entering NDD facilities must wear an identification badge.

2. External individuals to the Company must be identified at reception, and their entry into NDD facilities will be granted upon authorization and accompanied by a Company employee.

3. Any computer or notebook leaving NDD premises will require prior authorization from the responsible manager.

4. NDD service providers are responsible for actions or damages caused by their employees to NDD's assets and must also ensure the confidentiality of accessed information.

5. Documents or papers containing confidential information, when no longer needed, must be shredded or destroyed to prevent reading.

6. Read-only media (CD-ROMs, CD-Rs, DVDs, etc.) containing confidential information, when no longer needed, must be broken or destroyed to prevent misuse.

7. Rewritable media (HD or SSD drives, pen drives, SD cards, tapes, CD or DVD RW discs, or similar) containing confidential information, when no longer needed, must be securely erased using the appropriate procedure indicated by the Information Security team before reuse or disposal.

8. Equipment and their internal components will be periodically inventoried, and only authorized employees can rearrange equipment and parts.

Access Credentials

1. Access credentials, identifications, and passwords must be individual and kept confidential, not to be transferred or shared.

2. Each employee will systematically and automatically change their password, with a maximum validity of 42 (forty-two) days, and it is their responsibility to choose strong, complex, and long passwords.

3. Passwords must be different across the systems used, and they must contain numbers, uppercase and lowercase letters, and special characters.

4. NDD adopts the concept of least privilege, where employees should only have access to information strictly necessary for the fulfillment of their duties.

5. Access granting and revocation processes are the responsibility of the SRE (Site Reliability Engineering) and IT Infrastructure teams and must be centralized in these teams and executed according to documented flows.

Network Usage

1. Internet access is provided for Company activities and purposes. Legal personal use may occasionally be permitted, preferably outside working hours, provided it does not violate other rules.

2. It is prohibited to use the network to access or send pornographic, offensive, or defamatory content, as well as to harass third parties, whether employees or not.

3. The use of social networks such as Facebook or Twitter and video sites like YouTube, Vimeo, and Netflix during working hours is considered inappropriate and may be blocked at any time at the Company's discretion.

4. Any known sites with prohibited or inappropriate content may be on automatic blocking lists. Any errors in the classification of a particular site can be reported to the proxy team for rectification.

5. Internet access may and will be monitored and recorded by the Company. Records are available to the Company for as long as it deems necessary.

6. It is not allowed to install, use, or configure equipment (hardware or software) that provides access to the corporate network without formal authorization and knowledge of the Information Security Team. Specifically, the installation of Wi-Fi access points, Bluetooth devices, modems, hubs, switches, VPNs, routers, or remote access software for personal use is not allowed.

7. Corporate email is maintained by NDD and must have anti-spam protection permanently active.

8. All messages sent via email with the professional address are the property of the Company, therefore they should be used for NDD-related matters, and no expectation of privacy should be maintained regarding their contents.

9. Sending or participating in chains, even those of solidarity, prizes, or information, using the corporate email provided by NDD is prohibited.

10. Sending messages with electoral, defamatory, offensive, prejudiced, obscene, pornographic content, or content that could be interpreted as racial, sexual, religious, or political discrimination is prohibited.

11. Distributing, via email, discussion groups, forums, and similar forms of communication, unsolicited "chain" messages and mass, commercial, political propaganda, or unsolicited email is not allowed.

12. Notebooks, laptops, tablets, and other personal or third-party equipment must not be directly connected to the Company's network without authorization. Such authorized equipment can be connected to the Wi-Fi network and have access to internal services via VPN managed by the Company.

Station and Server Protection

1. All NDD computers and servers must have antivirus software installed.

2. Users must not prevent the operation and updating of antivirus software without authorization and knowledge of the antivirus administration team.

3. If any problems are identified with the antivirus software, the user must immediately notify the Infrastructure team, which will take appropriate action.

4. All NDD computers and servers must have monitoring agents installed, which must not be uninstalled without authorization from the Infrastructure and Information Security team.

Program Usage

1. As Workstations are provided with the minimum necessary programs - operating system and applications - for performing their basic function at NDD.

2. Installed and used software must comply with their usage licenses and not contravene other NDD rules and regulations.

3. Installation of any software, free or paid, on NDD equipment without authorization from the Infrastructure and Information Security team is not permitted. If you need specific software, contact us through an open ticket on the Helpdesk portal (clicando aqui).

4. Using or installing software without a usage license or in someone else's name without authorization constitutes piracy, with the user and installer subject to administrative, legal, and criminal penalties under the law.

5. Periodic checks will be carried out on equipment inventory, regarding both hardware and software, to identify deviations from the rules.

Backup

1. Each user is responsible for backing up their work files on Sharepoint and file systems provided by NDD.

2. Files generated on workstations must be saved on Sharepoint because backups are only performed there, and in case of accidental deletion, they can be quickly recovered. If a file or folder is saved only on the computer and there is an accidental deletion, it cannot be recovered.

3. Copying confidential data for processing or storage on external services, unauthorized third parties by NDD or its clients, is not allowed.

4. Whenever possible, confidential data should be encrypted in backups.

5. Every backup must undergo periodic restoration testing.

6. Storage media must be kept in a secure location, such as a cabinet, cloud, safe, or room with a key or access control, and manufacturer-suggested lifetimes must be respected.

7. Some backups have a predetermined lifespan by law, so the responsible backup team must be informed and ensure they are available during that time, as well as the necessary equipment for their recovery when needed.

Systems and Applications

1. Transfer of data for processing or storage on external services, third parties not expressly authorized by NDD or clients, is not allowed.

2. Storage and transfer of confidential data must always be encrypted using mechanisms approved by the Company.

3. NDD will preferentially choose solutions/applications that use secure protocols, both in data transfer and storage. Applications that do not use these features must be validated by the information security team before use begins.

4. A NDD will preferably opt for the use of dual or multi-factor authentication systems (MFA/2FA). Applications that do not utilize these features must be validated by the information security team before their use.

5. Systems should generate security event logs. Functions of the security system in use, operating system resources, database resources, and/or application resources should be used for this purpose. Logs should contain at least the following information:

- Application and function identification;
- Occurrence timestamp;

- Information identifying the machine or location of the occurrence;
- Relevant data manipulated by the application.

The Security System may handle the logging of some of this information.

6. No In the development and maintenance of systems, the use of approved software and file control and versioning repository (such as sources, models, documents, diagrams, web pages) is mandatory.

7. Each developer is responsible for the integrity of the system files they are working on, preferably using designated server workspaces.

8. Every application developer must follow, when available and applicable, security recommendations for development.

Server Administration

1. All new server installations must follow standard procedures and include mandatory packages, Service Packs, and Hot Fixes.

2. Security update installations must be performed by the direct responsible of each server, following security guidelines regarding backup before the procedure, timing adequacy, and fault recovery plan.

3. Acessos Remote accesses must always use encrypted mechanisms. Remote access services that do not use encryption should be disabled.

4. Used equipment must have an updated operating system with deployed security features.

5. The activation of new network services will be conditioned to a risk analysis (to be carried out by the Security and Infrastructure Team), where at least the following aspects will be considered: service security requirements, objective, service target, access form, administration form, and traffic volume.

6. The installation of network services not authorized by the Security and Infrastructure Team is not allowed.

7. All shared information traffic must be protected through encryption.

8. The Information Security team may indicate and use intrusion detection and prevention tools to issue alerts and record possible intrusion attempts.

Secure Development

1. Develop according to SDL (Security Development Lifecycle) best practices, OWASP (Open Web Application Security Project) TOP10, and SANS TOP25.

2. Develop by applying Privacy by Design and Privacy By Default principles, aiming for the security and protection of treated data.

3. Train the development team for secure development practices.

4. NDD has an internal policy specifically for the secure development of its products following market best practices.

Records and Audits

1. Os Administrators must enable security logs whenever possible to assist in analysis in case of potential failures and/or during audits.

2. Security logs should be periodically analyzed (manually or automatically).

Approvers:
DIRECTION