



Information Security Policy

The IT Security Policy identifies the rules and procedures for all individuals accessing and using the companies' IT assets and resources. The objective of this policy is the preservation of confidentiality, integrity, and availability of systems and information used by organization members.

All employees must, as a minimum, meet the requirements set out in this Policy. In any country where the requirements of applicable laws, directives or practices establish a higher standard, employees must meet those standards.

Table of Contents

Overview.....	3
Foreword.....	3
Objectives.....	3
Definition.....	3
Responsibilities.....	4
Acceptable Use Policy.....	5
Disciplinary Action.....	5
Data classification.....	5
Sensitive Data.....	6
Protection.....	6
Access.....	6
Logon and logoff.....	6
Password Policy.....	7
Computer viruses, worms and Trojan horses.....	7
Encryption.....	8
Portable device and media.....	8
USB Storage Device.....	8
Email Usage.....	8
Sharing and forwarding.....	8
User Identity.....	9
Content of Message.....	9
Public Representations.....	9
Incidental Disclosure.....	10
Bring Your Own Device.....	10
Physical Security.....	10
Disposal of Media & Equipment.....	11
Security Awareness and Procedures.....	11
Security Review Plan.....	11
Independent Security audit.....	11
Updates on gaming services.....	11
Social Media.....	12
Network & Remote Access.....	12
Incident Response Plan.....	12
Network Security.....	13
Location Service for Company Devices.....	13
Clear Desk Policy.....	13
Use of Artificial Intelligence.....	13
Corporate Assets Acceptable Use Policy.....	14
Authorized Use.....	14
Compliance with Laws and Policies.....	14
Security and Protection.....	14
Communication of Policies.....	15

Overview

Foreword

The present document encompasses all aspects of security surrounding Company information (confidential or not) and is meant to establish management direction, procedural requirements, and technical guidance required to ensure the appropriate protection of Company information systems. This document, along with the other policy and procedure documents are to be reviewed by the Company management on an annual basis or whenever significant changes take place. Before any new updates take place, these will be reviewed and approved by a CEO or the Board of Directors. This policy is distributed to all Company employees (including contractors) that must read this document in its entirety and acknowledge it by signing the form confirming they have read and understand this policy fully (either during the onboarding process for new employees, or when there are significant updates relevant to the employees in the document).

Objectives

The objectives of this policy are to safeguard the integrity, confidentiality and availability of all the Information handled by Company, by making sure that:

- The Information Security Policy provides clear direction for the information security program. The Information Security Policy shows that management is committed to information security.
- Management supports the organization's information security policy.
- The Information Security Policy shows that management is prepared to support an on-going commitment to information security.
- The Information Security Policy is consistent with the business objectives.
- The Information Security Policy meets the organization's business requirements.
- The Information Security Policy complies with all relevant laws and regulations Company is subject to.

Definition

For clarification purpose, some terms used in this document are defined below:

- "Company" or "The company" should be understood as Next To You B.V..
- "Employees" should be understood as all employees of the Company as well as 3rd party individuals engaged with the company through a service or other type of agreement.
- "Sensitive data" shall refer to any type of data, in whatever form, owned by the Company, or shared with any 3rd party, and that is not public or common knowledge. Thus including, but not limited to, personal data as defined by the GDPR, but also Company financial, contractual and legal data.

Responsibilities

The CEO (Chief Executive Officer) of the Company or the Head of the IT department has been entrusted with direct responsibility for maintaining this policy and providing advice on information security and guidance on its implementation.

- Data/information obtained inappropriately should not be used;
- Finding a system weakness should be reported immediately and should not be taken advantage of;
- Every employee has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the company's information system;
- When the confidentiality of information is unclear, its classification should be ascertained; and
- Report any known violation or system weakness to the person or persons responsible for security Information Security Policy.

The company handles personal and sensitive data daily. Information must have adequate safeguards in place to protect them, to protect player and employee privacy, to ensure compliance with various regulations and to guard the future of the organization.

All employees have a responsibility to conduct themselves in an ethical manner. In particular:

- Handle Company and customer information in a manner that fits with their sensitivity; Limit personal use of the company information and telecommunication systems and ensure it doesn't interfere with your job performance;
- The Company reserves the right to monitor, access, review, audit, copy, store, any electronic communications, equipment, systems and network traffic for audit purpose;
- Do not use email, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personal information unless authorized in writing;
- Protect sensitive information;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorized software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, in accordance with the Incident Response Policy.
- Do not disclose any sensitive information, whether handled by Company or entrusted by a 3rd party.
- Do not engage, or otherwise use Company Information System, in hacking activities that include, but are not limited to, gaining unauthorized access to any information system (Managed by Company or not), altering, damaging or otherwise obtaining password, encryption or other mechanism that could grant unauthorized access.
- Do not test or attempt to compromise any information system unless specifically authorized to do so by the management. Employees must not possess software or other tools that are designed to compromise information security.

It is a shared responsibility of ensuring Company systems and data are protected from unauthorized access and improper use. If you need clarification or have any question on any of the policies detailed herein, please seek advice and guidance from your line manager.

Acceptable Use Policy

Management is committed to protecting the employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes cardholder data.
- Employees should ensure that technologies should be used and set up in acceptable network locations.
- Keep passwords secure and do not share accounts. Only use the password management system provided by the Company. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops, workstations, mobile and tablet should be secured with a password-protected screensaver with the automatic activation feature.
- All password/PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, particular care should be exercised.
- Unless duly authorized by management, postings by employees from a company email address or account to newsgroups, forums or any social media is strictly prohibited.
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee may result in disciplinary action, from warnings or reprimands, including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

Data classification

Data and media containing data must always be labeled to indicate sensitivity level:

- Public: Information is not confidential and can be made public without any implications from the Company.
- Internal Use: Information is restricted to the Company and can freely be shared across employees in a direct agreement with the Company.

The data should however be protected from other external access and shall not be disclosed externally without prior written consent of the Company.

- Confidential: Any information for which there are legal or strategic requirements for preventing disclosure or financial penalties for disclosure. Confidential data includes data collected by the Company and tied to a privacy statement.

Wherever possible, data and media containing confidential data must be labeled to indicate sensitivity level.

Whenever documents are not marked, for instance when the data direct labeling is not practically possible, the policy should still be enforced, and notably through a more restrictive access policy.

In addition to the above, the following classification should be applied by default:

- Business peer-to-peer communication such as, but not limited to, email and chat should be considered “Shared” unless otherwise specified.
- Any document produced by the Company should be considered “Internal Use” unless otherwise specified.
- Any document containing Personally Identifiable Information (In the sense of the GDPR), whether it is the Company’s customers or employee’s data, should be considered “Confidential”.

Sensitive Data

Protection

All sensitive data stored and handled by Company and its employees must be securely protected against unauthorized use at all times. Any sensitive data that is no longer required by the Company for business reasons must be discarded in a secure and irrecoverable manner.

- If there is no specific need to see personal or sensitive data, it must be masked when displayed.
- Company employees must not disclose sensitive data outside the Company premises and messaging systems (Chat, Mail, Skype, etc.), unless duly authorized to do so in writing by the management.

Any confidential documents should be stored in a safe place, or in a cabinet which is locked and only accessible to authorized people.

Access

All access to sensitive data should be controlled and authorized. Access to sensitive data is granted to individuals according to their role.

No one is authorized to keep confidential data stored out of Company drives. It is prohibited to:

- Store any sensitive data under personal Drive.
- Store any sensitive data out of the Company related drive. It is mandatory to inform if you have access to data that does not correspond to you.

The Company reserves the right to make periodic reviews of personal drives and messaging applications without prior notice. It's the employee's obligation to store the sensitive data and the non-sensitive but important data in the corresponding drive.

Logon and logoff

All users must be positively identified prior to being able to use any Company computer or communications system resources.

In case of rooms with single occupations, the room must be locked. In case a user forgets to lock their computer, if there has been no activity on a computer terminal, workstation, or personal computer for a certain period, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room badge readers, or similar technology. All other users must lock their computer whenever they leave their desk.

Using someone else's credentials to connect is strictly prohibited. In particular, using a workstation logged with such an account is not permitted.

Password Policy

With the exclusion of service accounts, the following policy should be applied for Company accounts.

- The password should contain a minimum of 8 characters.
- Password complexity requirements should be enabled whenever possible (usually at least one upper case letter, one number and one symbol).
- The password maximum age is 90 days and a previous password cannot be reused.
- The password must not be the same as the username.
- In the event of 3 consecutive failed login, the related account should be locked out for a minimum of 10 minutes.

Computer viruses, worms and Trojan horses

Approved and current virus-screening software must be enabled on Company's computer systems. This software must be used to scan all software coming from third parties or other departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

The willful introduction of computer viruses or disruptive/destructive programs into the Company environment is prohibited, and violators may be subject to prosecution. The IT department is responsible for eradicating viruses from all computer systems. As soon as a virus is detected, the involved user must immediately notify the IT department to assure that no further infection takes place and that any expertise needed to eradicate the virus are promptly engaged.

The Company's computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless tested and approved by the IT Department.

Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Encryption

When sensitive information is transmitted over any communication network, it must be sent in encrypted form. Whenever information is stored or transported in computer-readable storage media, it must also be in encrypted form.

Encryption of information in storage or in transit must be achieved through commercially available products approved by the IT department.

Encryption keys used for Company information are always classified as Confidential information. Access to such keys must be limited only to those who have a need to know. Unless the approval of the CTO or the maximum responsible of the IT team, is obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or other third parties.

Wireless networks in use must always be configured to employ encryption.

Any form of sensitive or transactional data transmitted from/to the online system must be encrypted.

Portable device and media

Users in the possession of portable, laptop, notebook, handheld, and other transportable computers and/or media containing sensitive information, must not leave these computers/media unattended at any time unless the information is stored in encrypted form.

Users in the possession of transportable computers containing unencrypted confidential data must not check these computers in airline luggage systems or with hotel porters. These computers must remain in the possession of the traveler as hand luggage.

USB Storage Device

The usage of USB storages including, but not limited to, USB keys and USB Hard drives, is not authorized.

Email Usage

Sharing and forwarding

Electronic mail accounts, like user IDs, are for specific individuals and must not be shared. If a user goes on vacation or is otherwise unable to check their mail for

extended periods, mail can be forwarded to another Company employee with the exclusion of 3rd parties. Notices can be established that will automatically inform correspondents that the recipient will not be responding for a certain period of time. Upon departure from the Company, the employee's electronic mail account must be terminated, and email erased. The mail accounts of directors or employees that receive critical business information may be maintained for a transition period of 3 months.

If an electronic mail message contains sensitive information, users must not forward it to another recipient unless the other recipient is known to be authorized to view the information, or the originator approves the forwarding. Broadcast electronic mail message facilities must not be employed unless department manager approval is obtained, but the use of selected distribution lists (if these exist) is both advisable and permissible without such approval.

User Identity

Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

With the exception of a generic email, such as customer support services that may be anonymous, users must not send anonymous electronic communications. At a minimum, all users must provide their name and phone number in all electronic communications. Electronic mail signatures indicating job title, company affiliation, address and other particulars are strongly recommended for all electronic mail messages. Digital certificates are also recommended for electronic mail.

Content of Message

Users must not use profanity, obscenities, or derogatory remarks in any electronic mail messages discussing employees, customers, competitors, or others involved with Company business. Such remarks may create legal problems such as trade libel and defamation of character. Special caution is warranted because backup and archival copies of electronic mail made by third parties may be more permanent and more readily accessible than traditional paper communication.

Public Representations

No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voicemail message, or any other public representation about the Company may be issued unless prior approval has been granted by the authorized management. The Company, as a matter of policy, does not send unsolicited electronic mail, nor does it issue unsolicited fax advertising. Nobody outside the Company may be placed on an electronic mail distribution list without indicating their intention to be included on the list through an opt-in process.

If Company users are bothered by an excessive number of unwanted messages from a particular organization or electronic mail address, they must not respond directly to the sender. Recipients must forward samples of the messages to the IT helpdesk support for resolution. Users must not send a large number of messages in order to overload a server or user's electronic mailbox in retaliation for any perceived issue.

Incidental Disclosure

Company information systems must not be used for the exercise of a user's right to free speech. Sexual, ethnic and racial harassment, including unwanted telephone calls, electronic mail and internal mail, is strictly prohibited. Users must respond directly to the originator of offensive electronic mail messages, telephone calls, or other communications. If the originator does not promptly stop sending offensive messages, users must report the communications to their manager and to Human Resources.

Bring Your Own Device

The Company allows the use of personally owned devices (non-corporate devices) in the company context as long as the devices follow the same rules and practice than described in:

- Acceptable use policy
- Data classification
- Protect stored data
- Logon and logoff process
- Computer viruses, worms and Trojan horses
- Encryption
- Portable device and media
- Disposal of media & equipment

However, such usage is under the employee's responsibility to make sure to respect the aforementioned rules and practice. Failing to comply may result in the same disciplinary action as defined in this document "Information Security Policy".

Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to Confidential or Internal Only data.
- Employees should ensure that technologies should be used and set up in acceptable network locations.
- A list of Company devices should be maintained.
 - The list should include make, model and location of the device
 - The list should have the serial number or a unique identifier of the device
 - The list should be updated when devices are added, removed or relocated
- Personnel using the devices should verify the identity of any 3rd party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel.
- Media containing sensitive data information must be handled and distributed in a secure manner by trusted individuals.
- Strict control is maintained over the external or internal distribution of any media containing sensitive data and must be approved by management.

- Strict control is maintained over the storage and accessibility of media
- All computers that store sensitive data must have a password protected screensaver enabled to prevent unauthorized use.

Disposal of Media & Equipment

Should any media that is no longer required due to numerous reasons, such as excess of useful life, change in requirements, damage, inability to upgrade, non-viable maintenance cost or simply replacement by new hardware must be checked by the IT department to ensure that no sensitive information is held on the device.

If the item is non-salvageable i.e. no parts can be used for other maintenance purposes, the IT department would need to dispose of the equipment. The members of the IT department would need to ensure that data is erased from the equipment by securely overwriting the data, while the CTO, or the employee responsible for the IT team would need to authorize the release of the equipment.

The disposal of the equipment can:

- Bin
- Sold to employees
- Given to recycling companies

Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain security awareness. The protection of sensitive data demands regular training (annually) of all employees, including service contractors that access sensitive data.

- Company security policies must be reviewed annually and updated as needed.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.

Security Review Plan

Security reviews will be organized and performed by the IT team to make sure that the security policies and procedures are being fulfilled.

Independent Security audit

A third-party company will carry out an annual security review, providing an official report with the non-conformities that will be reported by the Company to the authorities.

Updates on gaming services

Critical gaming services are identified by the DevOps team of the IT department. Each month available updates will be manually checked by the System Administration team and when an update is stable, he or she will find the next best schedule, working in collaboration with the Product team to apply the update. If downtime is expected, it will be communicated to the rest of the company and customers.

Social Media

Should the Company make use of social media on the internet (Skype, Facebook, Twitter, etc.). This should only be done for business use and no confidential information should be disclosed over this medium. The Company may decide at any time, to keep logs of chats and activities carried out using this medium.

Network & Remote Access

All Company employees, including service provider employees, may be granted remote access (VPN).

- It is the responsibility of the employees, contractors, vendors and agents with remote access privileges to the Company network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Company.
- All hosts that are connected to the Company internal networks via remote access technologies will be monitored on a regular basis.

With the exclusion of the "Guest Wifi", access to the network is strictly reserved to Company managed devices, unless otherwise approved by the Company management in writing.

Incident Response Plan

Security incident means any incident (accidental, intentional or deliberate) relating to the Company communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.

The Incident response plan must be tested once annually. Copies of this incident response plan are to be made available to all relevant staff members and take steps to ensure that they understand it and what is expected of them.

- Employees of the Company will be expected to report to the CTO or the head of the IT team for any security related issues.
- Each department must report an incident to the CTO (preferably) or to another member of the IT team.
- The IT Team will investigate the incident and assist the potentially compromised department in limiting the exposure of sensitive data and in mitigating the risks associated with the incident.
- The IT Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident to the regulator whenever appropriate.
- The IT Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
- If an unauthorized access is identified or detected as part of the quarterly test, this should be immediately escalated to the CTO or a member of the IT Operation Team that has the authority to stop, cease, shut down, and remove the offending device immediately.

- A department that reasonably believes it may have a leak of data, or a breach in any of the Company systems, must inform the CTO or the maximum responsible of the IT team. After being notified of a compromise, the IT Team will implement the Incident Response Plan.

The Company Security Incident Team is composed of:

- CEO or CTO
- The Devops Team

Network Security

Firewall protection shall be put in place to safeguard the company against unauthorized intrusion attempts. Wireless networks shall be password protected and used solely by the Company staff. Should guests wish to utilize an internet connection, a separate wireless connection shall be put in place, which is segregated from the Company network.

Location Service for Company Devices

The Company may collect and monitor location data of all company-owned devices (including laptops, smartphones, tablets, and other equipment) to safeguard corporate assets, support loss prevention and recovery, verify compliance with travel-related policies, and ensure user safety in emergency situations. Location data will be accessed only by authorized personnel, retained no longer than necessary for its intended purposes, and handled in accordance with applicable privacy laws and our Data Classification and Retention policies. Users will be notified that their devices are subject to location tracking as a condition of device issuance.

Clear Desk Policy

Outside of regular working hours, all workers must clean their desks and working areas such that all sensitive or valuable data is properly secured.

Use of Artificial Intelligence

- Purpose

The purpose of this policy is to establish clear guidelines for the use of Artificial Intelligence (AI) technologies within the organization. This policy aims to ensure that AI tools and systems are used securely, ethically, and in compliance with legal requirements while protecting the confidentiality, integrity, and availability of organizational data.

- Scope

This policy applies to all employees, contractors, consultants, and other personnel who use AI technologies or systems within the organization. This includes any AI-powered applications, tools, and services that process or interact with organizational data.

- General Guidelines

Authorized Use: Users are only authorized to use AI systems, tools, and applications approved by the organization's IT and security teams.

Data Security: All AI applications must comply with the organization's data security protocols. Users must ensure that AI tools are not used to process or store sensitive or confidential information.

Privacy Compliance: AI systems must adhere to all applicable privacy laws and regulations, including GDPR, HIPAA, or other relevant laws based on geographical location and industry.

Data Input and Output: Users must verify the accuracy and legitimacy of data input into AI systems to prevent bias, errors, or harmful outcomes. Users must also ensure the responsible use of AI-generated output and avoid making critical decisions based solely on AI results without human oversight.

- **Security Considerations**

AI systems and tools must be secured with appropriate authentication and access control mechanisms.

- **Ethical Use of AI**

Critical decisions (such as hiring, budget approvals, etc.) should not be solely based on AI recommendations. There must always be human oversight in the decision-making process.

- **Prohibited Uses**

Inappropriate Data Usage: The use of AI tools to process, analyze, or share data that violates the organization's policies on privacy, security, or compliance is strictly prohibited.

Unapproved AI Systems: Using AI systems or applications that are not vetted or approved by the organization's IT and security teams is not allowed.

- **Training and Awareness**

User Training: All users must complete periodic training on the secure and ethical use of AI technologies. This training will cover topics such as security protocols, privacy concerns, ethical considerations, and best practices.

- **Incident Reporting**

AI Security Incidents: Any security incidents or issues related to AI systems, such as data breaches, suspicious activities, or misuse of AI technologies, must be reported immediately to the IT security team using the organization's incident response procedures.

Corporate Assets Acceptable Use Policy

Authorized Use

Corporate assets should be used solely for legitimate business purposes in support of job responsibilities, projects, or activities approved by the Company.

Compliance with Laws and Policies

Employees must comply with applicable laws, regulations, and company policies when utilizing corporate assets, including but not limited to intellectual property rights, data privacy, the present information security, and software licensing agreements.

Security and Protection

Users are responsible for protecting corporate assets from unauthorized access, damage, theft, or misuse. Employees may be held financially responsible for any damage, theft, or loss of corporate assets incurred through their actions or negligence.

This policy aims to promote a culture of accountability and responsible asset management within the organization. By assigning a portion of the financial burden to employees, we ensure the fair allocation of costs and encourage vigilant usage and protection of corporate resources.

Communication of Policies

The Company shall ensure that employees read the company policies and procedures upon starting work with the Company, and after material change of the policies, and sign an acknowledgement for these policies and procedures.