

INFORMATION SECURITY POLICY

DEEP DIVE TECH BV

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

Contents

1. INTRODUCTION	4
2. SCOPE	4
3. POLICY DETAILS.....	4
4. RESPONSIBILITY	5
5. INFORMATION CLASSIFICATION	6
6. PROPERTIES TO SECURE.....	7
6.1. User ID.....	7
6.2. Passwords	7
6.2.1. User ID & Passwords	7
6.2.2. Password Management.....	7
6.2.3. Password Construction Requirements.....	8
6.3. Network.....	8
6.3.1. Internal Network Connections	8
6.3.2. External Network Connections	9
6.3.3. External Wireless Network.....	9
6.3.4. Network Connections	9
6.3.5. Remote Access	9
6.3.6. Internet Access.....	9
6.4. Antivirus	10
6.5. Portable Computers and Media	10
6.6. Equipment, Media and Data Disposal	10
6.7. Physical Security to Control Information Access	11
6.7.1. Backups.....	11
6.7.2. Formal Change Control.....	11
6.7.3. Development Conventions	11
6.7.4. Adequate Licenses'	12
6.7.5. Unauthorized copies.....	12
6.7.6. Backup Responsibilities	12
6.7.7. External Disclosure of Security Information	12
6.7.8. Personal Use.....	12

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

6.7.9.	Unbecoming Conduct	12
6.7.10.	Security Comprise Tool	13
6.7.11.	Prohibited Activities	13
6.7.12.	Security Incidents in Gaming System	13
6.7.13.	Mandatory Reporting.....	13
7.	TRAINING, OBLIGATIONS AND RIGHTS.....	13
7.1.	Training.....	13
7.2.	Responsibilities.....	14
7.3.	Rights	14
7.4.	Duties.....	14

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

1. INTRODUCTION

This policy refers to all information systems that are used by Deep Dive Tech BV. The purpose of this policy is to prevent unauthorized use, modification, disclosure, or destruction of all applications, data, and network resources used by Deep Dive Tech BV.

2. SCOPE

This policy applies to all information systems, including but not limited to applications, data, network resources, and hardware, used by or on behalf of Deep Dive Tech BV. It encompasses all employees, contractors, and affiliates who access, use, or manage these systems.

The purpose of this Information Security Policy is to:

- Prevent unauthorized access, use, modification, disclosure, or destruction of all applications, data, and network resources owned or managed by Deep Dive Tech BV.
- Ensure the confidentiality, integrity, and availability of Deep Dive Tech BV's information assets.
- Protect the interests of Deep Dive Tech BV, its customers, employees, and partners.
- Comply with applicable legal, regulatory, and contractual obligations related to information security.

3. POLICY DETAILS

- Access Control: Access to Deep Dive Tech BV's information systems shall be granted based on the principles of least privilege and need-to-know to perform job responsibilities. User access shall be reviewed and updated regularly to ensure ongoing relevance.
- Data Protection: Deep Dive Tech BV shall implement appropriate measures to protect data against unauthorized access, disclosure, alteration, or destruction. This includes encryption, secure data storage, and data masking where necessary.
- Incident Response: Deep Dive Tech BV will maintain an incident response plan to promptly and effectively respond to potential security incidents. Employees are required to report any suspected security incidents immediately.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

- **Employee Training:** All employees will receive regular training on information security, emphasizing their roles and responsibilities in protecting the organization's information assets.
- **Physical Security:** Physical access to critical information systems and infrastructure shall be controlled and monitored. Measures shall be in place to protect against unauthorized entry and environmental hazards.
- **Network Security:** Network infrastructure and services shall be designed, implemented, and maintained to ensure security, resilience, and reliable operation. Regular security assessments and monitoring will be conducted to detect and respond to potential vulnerabilities.
- **Compliance and Auditing:** Deep Dive Tech BV will regularly review and audit its information security practices to ensure compliance with this policy and relevant legal and regulatory requirements. Audit findings shall be addressed promptly to mitigate any identified risks.

4. RESPONSIBILITY

Deep Dive Tech BV holds direct responsibility for maintaining the Information Security Policy and providing advice and guidance on information security and its implementation.

All employees of Deep Dive Tech BV and any third parties are required to act ethically regarding information security. Specifically:

- Information obtained inappropriately must not be used or disclosed.
- Discovering a system's weakness is not an opportunity for exploitation but should be promptly reported.
- Each user is responsible for conducting their work with diligence and will be held accountable for any misuse of the company's information.
- When the confidentiality status of information is uncertain, its classification must be clarified.
- All known violations or system weaknesses should be reported to the designated authority.

Line Managers are tasked with authorizing access requests, ensuring they align with business needs and organizational security policies.

The HR department plays a crucial role in initiating new user access requests, user agreements, and providing information security training.

Asset owners must authorize access to their information assets, ensuring compliance with the asset's security requirements.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

All employees who handle data are expected to:

- Treat all data with the utmost sensitivity.
- Refrain from using company resources for any offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing, or illegal activities.
- Avoid disclosing personal information unless explicitly authorized.
- Maintain the security of passwords and accounts.
- Seek approval from the IT department before implementing any new software, hardware, or third-party connections.
- Avoid installing unauthorized software or hardware without explicit management approval.
- Keep desks clear of sensitive data and ensure computer screens are locked when unattended.
- Report any information security incidents to the IT department without delay.

5. INFORMATION CLASSIFICATION

Deep Dive Tech BV acknowledges the necessity of differentiating data protection levels to maintain data confidentiality. We have instituted data classification policies to ensure that each data type receives appropriate protection:

- Highly Sensitive Information: This category encompasses data that is paramount in sensitivity and value to Deep Dive Tech BV. Unauthorized access, usage, or disclosure could lead to substantial financial loss or reputational harm. Such information includes, but is not limited to, financial records, passwords, customer details, trade secrets, and sensitive source code. Access to this information is stringently controlled and is only provided on a need-to-know basis, adhering to the principle of least privilege.
- Sensitive Information: This category covers confidential data that does not rise to the level of highly sensitive information. It includes personally identifiable information (PII), intellectual property, and financial records that are not public. Access to sensitive information is confined to designated Deep Dive Tech BV employees who need this information to execute their duties.
- Internal Information: This category is designated for information used solely within Deep Dive Tech BV and not disclosed externally. It includes internal protocols, procedural documents, and non-sensitive employee information. Access to internal information is restricted to authorized personnel.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

- Public Information: This category includes information that is not confidential and can be freely shared. Examples are press releases, company brochures, and marketing materials available to the public.

6. PROPERTIES TO SECURE

6.1. User ID

Each staff member has a unique User ID to access the back office system. Generic User IDs are not allowed.

6.2. Passwords

Passwords are personal and must be kept secure by each system user. However, it is allowed for employees, to use company granted password protection software, that enable encrypted storage of passwords accessible by personal user ID and password.

6.2.1. User ID & Passwords

To implement the need-to-know process, Deep Dive Tech BV requires that each staff member accessing any system must have a unique and private password. These user IDs must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each staff member is personally responsible for the usage of his or her user ID and password.

6.2.2. Password Management

Passwords are an important aspect of our computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of the entire network. As such, all Deep Dive Tech BV's employees (including contractors and vendors with access to our systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

- All systems-level passwords must be changed at least every 90 days.
- All user-level passwords (e.g. Office 365, back office, etc.) must be changed at least every 90 days and cannot be reused with the past 3 passwords.
- Admin accounts to systems where Multifactor authentication is available must be used.
- Users should always use a different password for different systems.
- Passwords must not be inserted into email messages or other forms of electronic communication.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

- The only password manager system accepted to be used by Deep Dive Tech BV Employees is LastPass Premium
- All level passwords used must conform to the guidelines described below.
- Remember password option is not to be used.

6.2.3. Password Construction Requirements

Minimum length:

- 8 Character Complexity:
- Password must include a lowercase letter
- Password must include an uppercase letter
- Password must include a number
- Password must include a special character

Originality:

- The password may not contain the username

Password Aging:

- Enforce password history for the last 3 passwords
- Passwords expire every 90 days Lockout:
- Account locks out after 3 failed login attempts

6.3. Network

All sensitive business documents, meaning content of confidentiality reserved for by Deep Dive Tech BV, MUST be stored in a designated location under appropriate user access structure. User access can only be granted to users by system administrator after approval from IT management.

6.3.1. Internal Network Connections

All computers that store information and that are permanently or intermittently connected to internal computer networks must have a password-based access control system. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system.

Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is again entered. Multi-user systems

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

must employ automatic log-off systems that automatically terminate a user's session after a defined period of inactivity.

6.3.2. External Network Connections

All in-bound session connections to Deep Dive Tech BV computers from external networks must be protected with an approved password access control system.

6.3.3. External Wireless Network

Guests visiting Deep Dive Tech BV offices may need to use internet via laptop etc. A guest Wi-Fi network is available for that, which is outside the internal network, but still has access to the internet. This Wi-Fi communication is also encrypted, and password protected.

6.3.4. Network Connections

Except for emergency situations, all changes to Deep Dive Tech BV computer networks must be approved in advance by the IT Manager. All emergency changes to networks must be made only by authorized users. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems.

6.3.5. Remote Access

When employees are working from outside the office, they are always to use the remote access VPN that is configured by the IT Department. For one to connect to the VPN one must use their User ID, Password and MFA code while they have configuration files setup on their devices. This connection establishes a safe and encrypted network tunnel to the office, while it gives them access to company systems and data.

6.3.6. Internet Access

All staff are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of management. Internet access is monitored to ensure that staff are not visiting sites unrelated to their jobs, and to ensure that they continue to follow security policies.

Employees are not allowed to represent Deep Dive Tech BV on Internet discussion groups and in other public forums, unless they have previously received top management authorization to act in this capacity. All information received from the Internet should be suspected until confirmed by reliable sources.

Employees must not place any work material on any publicly accessible computer system such as the Internet unless the posting has been approved by the management and key official.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

6.4. Antivirus

All computers are setup with an antivirus and configured in a way that they can only be disabled or removed from the antivirus admin console that is handled by the IT Department.

The antivirus admin console handles all updates on the devices, the monitoring, and the alerting. Any infected computers are instantly isolated from the internal network, and an alert is sent to the IT Department.

6.5. Portable Computers and Media

All computers must have appropriate access protection (e.g. passwords and encryption) and must not be left unattended in public places.

Computer equipment is vulnerable to theft, loss or unauthorized access. Always secure laptop and handheld equipment when leaving an office unattended. When travelling, the high incidence of theft makes it inadvisable to leave in cars or take them into vulnerable areas.

Users of portable computing equipment are responsible for the security of the hardware and the information it always holds. The equipment should only be used by Deep Dive Tech BV employees to whom it is issued. All the policy statements regarding the use of software apply equally to users of portable equipment belonging to Deep Dive Tech BV.

Users of this equipment must pay particular attention to the protection of personnel data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible.

6.6. Equipment, Media and Data Disposal

If, a machine has ever been used to process personal data as defined under the Data Protection Act or "in confidence" data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realize that data which may be sensitive is being stored automatically on their hard disk.

Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

Therefore, disposal should only be arranged through the IT Department, department, who will arrange for disks to be wiped.

Hardware that has been removed will be stored in a secure area. If the hardware does not contain any data, it will be destroyed and recycled.

If the hardware contains data, it will be demagnetized immediately after removal. When demagnetization is done the hardware will be destroyed and recycled.

6.7. Physical Security to Control Information Access

Access to every office, computer machine room, and other Deep Dive Tech BV work area containing sensitive information must be physically restricted to those people with a need to know. When not in use, sensitive information must always be protected from unauthorized disclosure. When left in an unattended room, sensitive information in paper form must be locked away in appropriate containers.

During non-working hours, workers in areas containing sensitive information must lock up all information. Unless information is in active use by authorized people, desks must be clear and clean during non-working hours to prevent unauthorized access to information. Employees must position their computer screens such that unauthorized people cannot look over their shoulders and see the sensitive information displayed.

6.7.1. Backups

All personal computer software must be copied prior to its initial usage, and such copies must be stored in a secure location. These master copies must not be used for ordinary business activities but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

6.7.2. Formal Change Control

All computer and communications systems used for production processing must employ a documented change control process that is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures. This policy applies to personal computers running production systems and larger multi-user systems.

6.7.3. Development Conventions

All production software development and software maintenance activities performed by in-house staff must follow policies, standards, procedures, and other systems development conventions. These conventions include proper testing, training, and documentation.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

6.7.4. Adequate Licenses'

Deep Dive Tech BV's management must make appropriate arrangements with software vendors for additional licensed copies, if and when additional copies are needed for business activities.

6.7.5. Unauthorized copies

Users must not copy software provided by Deep Dive Tech BV to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance permission from a responsible staff member. Ordinary backup copies are an authorized exception to this policy.

6.7.6. Backup Responsibilities

Personal computer users must regularly back up the information on their personal computers or ensure that someone else is doing this for them.

All backups containing critical or sensitive information must be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications that handle critical production information. It is the responsibility of the information owner to ensure that this plan is adequately developed, regularly updated, and periodically tested.

6.7.7. External Disclosure of Security Information

Information about security measures for Deep Dive Tech BV computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless approved by management. For example, publishing modem phone numbers or other systems that access information in directories is prohibited. Public disclosure of electronic mail addresses is permissible.

6.7.8. Personal Use

Deep Dive Tech BV information systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with productivity, and does not pre-empt any business activity. Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a luncheon.

Personal use that does not fall into these three categories requires advance permission.

6.7.9. Unbecoming Conduct

Deep Dive Tech BV Directors reserve the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of Deep Dive Tech BV information systems, which adversely affects the ability of others to use these information systems, or that, is harmful or offensive to others is not permitted.

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

6.7.10. Security Comprise Tool

Unless specifically authorized by the management, Deep Dive Tech BV employees or third-party contractors must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Without this type of approval, workers are prohibited from using any hardware or software that monitors the traffic on a network or the activity on a computer.

6.7.11. Prohibited Activities

Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the director. Incidents involving unapproved system hacking, password guessing file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered serious violations of Deep Dive Tech BV's internal policy. Short-cuts bypassing systems security measures, and pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

6.7.12. Security Incidents in Gaming System

Any abuse or exploitation which attempts to distort the result of a game or alter the pay-out should be considered a security incident; unfocussed, weak attacks on firewalls need not be treated as individual security incidents if they are effectively blocked by the existing precautions.

6.7.13. Mandatory Reporting

All suspected policy violations, security incidents, system intrusions, virus infestations, and other conditions that might jeopardize Deep Dive Tech BV's information or information systems must be immediately reported to the key official.

7. TRAINING, OBLIGATIONS AND RIGHTS

7.1. Training

All personnel at Deep Dive Tech BV will receive regular training on data classification policies and procedures to ensure they understand their responsibilities for data confidentiality and access control. The training will cover the different data classifications used by the company, the criteria for each classification, and the access controls and security measures in place for each type of data. Additionally, personnel

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025

will be trained on how to identify and report any suspected security breaches or incidents related to data classification

7.2. Responsibilities

All personnel at Deep Dive Tech BV have a responsibility to protect the company's data, regardless of its classification. Personnel are expected to adhere to the data classification policies and procedures in place, including proper handling and storage of data and adherence to access controls. Additionally, personnel must report any suspected security breaches or incidents related to data classification to the appropriate parties.

7.3. Rights

Personnel at Deep Dive Tech BV have the right to access data that they require to perform their job duties, provided they have the appropriate clearance and authorization for the data classification in question. Personnel also have the right to report any suspected security breaches or incidents related to data classification without fear of retaliation.

7.4. Duties

Personnel at Deep Dive Tech BV have a duty to protect the company's data and ensure that it is classified appropriately. Personnel must comply with data classification policies and procedures in place, including proper handling and storage of data and adherence to access controls. Personnel must also report any suspected security breaches or incidents related to data classification to the appropriate parties, as outlined in the company's incident response plan.

By providing regular training to personnel and outlining their responsibilities, rights, and duties related to data classification, Deep Dive Tech BV can ensure that all personnel are aware of their role in protecting the company's sensitive data. This helps to reduce the risk of unauthorized access or disclosure and ensures that all personnel are working together to safeguard the company's valuable assets.

Signature
Name
Role

Dmytro Strumilenko
Dmytro Strumilenko
Chief Technical Officer

Document	Owner	Version	Issue Date
Information Security Policy	Dmytro Strumilenko - CTO	1.0	23/09/2025