

Information Security Policy

1. Introduction

- 1.1. Mostbet88.com (hereinafter – “Website”) is owned and operated by Svideloco N.V. (hereinafter – “the Company”), a company registered and established under the Law of Curacao, registration number 161541, registered address: Trias Building, Hanchi Snoa 19, Willemstad, Curacao.
- 1.2. Svideloco N.V. is licensed and regulated by The Curacao Gaming Control Board.
- 1.3. In certain jurisdictions Svideloco N.V. is using NEVADIN LIMITED (a company registered and established under the Law of Cyprus, registration number: HE 433770, registered address: Agias Zonis & Thessalonikis, NICOLAOU PENTADROMOS CENTER, Floor 10, Flat/Office 1001A, BLOCK B, 3026, Limassol, Cyprus) as a payment agent.

2. Acceptable Use Standard

- 2.1. The purpose of this chapter is to outline the acceptable use of computer equipment and other electronic devices at the Company. These rules are in place to protect the employee and the Company. Inappropriate use exposes the Company to cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.
- 2.2. This chapter applies to the use of information, electronic and computing devices, and network resources to conduct the Company’s business or interact with internal networks and business systems, whether owned or leased by the Company, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at the Company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Company policies and standards, and local laws and regulation. This chapter applies to employees, contractors, consultants, temporaries, and other workers at the Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company.
- 2.3. General Use and Ownership
 - 2.3.1. The Company proprietary information stored on electronic and computing devices whether owned or leased by the Company, the employee or a third party, remains the sole property of the Company. You must ensure through



legal or technical means that proprietary information is protected in accordance with the data protection standard.

2.3.2. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of the Company's proprietary information.

2.3.3. You may access, use or share the Company's proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

2.3.4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

2.3.5. For security and network maintenance purposes, authorized individuals within the Company may monitor equipment, systems, and network traffic at any time.

2.3.6. The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.4. Security and Proprietary Information

2.4.1. System level and user level passwords must comply with the password policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

2.4.2. All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

2.4.3. Postings by employees from a Company email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is during business duties.

2.4.4. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

2.5. Unacceptable Use

2.5.1. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

2.5.2. Under no circumstances is an employee of the Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Company owned resources.

2.5.3. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use:



2.5.3.1. System and Network Activities. The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Company.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the end user does not have an active license is strictly prohibited.
- Accessing data, a server, or an account for any purpose other than conducting the Company's business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
- Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Company's account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the Company is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.



- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the Company's network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of the Company employees to parties outside the Company.

2.5.3.2. Email and Communication Activities. When using company resources to access and use the Internet, users must realize they represent the Company. Whenever employees state an affiliation to the Company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Company". The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the Company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Company or connected via the Company's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.5.3.3. Blogging and Social Media. Blogging or posting to social media platforms by employees, whether using the Company's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this chapter. Limited and occasional use of the Company's systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Company's policy, is not detrimental to the Company's best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from the Company's



systems is also subject to monitoring. The following activities are strictly prohibited, with no exceptions:

- The Company's Privacy Policy also applies to blogging. As such, Employees are prohibited from revealing any Company confidential or proprietary information, trade secrets or any other material covered by the Company's Privacy Policy when engaged in blogging.
- Employees may also not attribute personal statements, opinions or beliefs to the Company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of the Company. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Company's trademarks, logos and any other Company intellectual property may also not be used in connection with any blogging or social media activity.

3. Access Management

- 3.1. This chapter aims to establish a comprehensive framework for controlling and managing user access to the Company's systems, applications, and data resources. Also, this chapter aims to provide clear guidelines and procedures for granting, reviewing, and revoking access privileges, ensuring that users have the appropriate level of access based on their roles and responsibilities. This chapter seeks to minimize the risk of unauthorized access, data breaches, and insider threats by implementing effective access management practices. By implementing strong authentication mechanisms, role-based access controls, and regular access reviews, we strive to ensure that only authorized individuals can access sensitive information, protect the confidentiality and integrity of our systems and data, and comply with regulatory requirements. By prioritizing access management, we strengthen our overall cybersecurity posture, safeguard against unauthorized access, and maintain the trust and confidence of our stakeholders.
- 3.2. The Access Management applies to all Company's employees, contractors, and stakeholders. It encompasses managing and controlling user access privileges to systems, applications, and data resources within our IT infrastructure. This chapter covers all accounts and credentials to authenticate and authorize individuals' access. It sets forth guidelines for user provisioning, role-based access control, and segregation of duties to ensure appropriate access levels are granted based on job responsibilities and the principle of least privilege. The policy defines user account creation, modification, and termination procedures, as well as password management, session management, and access revocation. It also outlines the responsibilities of individuals involved in access management



processes, including system administrators, IT managers, and access administrators. Compliance with this policy is mandatory for all individuals within the Company, and any deviations or exceptions require approval from the designated authority responsible for access management and cybersecurity governance.

3.3. Safeguards

3.3.1. To achieve the Company's overall mission, and the purpose of this cybersecurity policy, the Company shall:

- AM-01 Define a process for creating and documenting roles and responsibilities for each of the Company's workforce members.
- AM-02 Ensure that the Company's documented roles and responsibilities for workforce members consider the principle of separation of duties when defining roles.
- AM-03 Maintain documented Access Control Lists (ACLs) for each computing system and business application system.
- AM-04 Ensure that the Company's documented Access Control Lists (ACLs) for computing systems and business applications are based on the Company's defined roles for workforce members.
- AM-05 Maintain Access Control Lists (ACLs) on computing system objects based on approved documentation, roles, and the principle of least privilege.
- AM-06 Maintain Access Control Lists (ACLs) on computing system functions based on approved documentation, roles, and the principle of least privilege.
- AM-07 Maintain Access Control Lists (ACLs) on code repositories based on approved documentation, roles, and the principle of least privilege.
- AM-08 Ensure that the Company's Access Control Lists (ACLs) enforce encryption of data at rest on each of the Company's computing systems.
- AM-09 Ensure that the Company's Access Control Lists (ACLs) enforce data encryption in transit on each computing system.
- AM-10 Define a process for reviewing the Company's documented Access Control Lists (ACLs) on a regular basis.
- AM-11 Define a process for reviewing the Company's Access Control List (ACL) documentation on a regular basis.
- AM-12 Define a process the Company shall use to regularly review the Company's group or role membership used by the Company's Access Control Lists (ACLs) regularly.
- AM-13 Ensure the Company's information systems log and alert changes to group or role memberships or configured Access Control Lists (ACLs).



- AM-14 Ensure the Company's information systems log and alert changes to group or role memberships or configured Access Control Lists (ACLs).

4. Data Inventory Management

- 4.1. Our Data Inventory Management policy aims to establish a comprehensive framework for identifying, classifying, and managing the data assets within our Company. This chapter aims to provide clear guidelines and procedures for documenting the types, locations, and sensitivity levels of our data and defining ownership and accountability. This chapter seeks to enhance data governance, protect sensitive information, and ensure compliance with privacy regulations and data protection requirements by implementing effective data inventory practices. Through regular data audits, mapping exercises, and classification standards, we strive to improve data visibility, enable effective data protection measures, and minimize the risk of unauthorized access or data breaches. By prioritizing data inventory management, we enhance our overall cybersecurity posture, reduce data-related risks, and maintain the trust and confidence of our stakeholders.
- 4.2. The Data Inventory Management policy applies to all our Company's employees, contractors, and stakeholders and encompasses the systematic identification, classification, and management of all data assets within our IT infrastructure. This policy covers all types of data, including sensitive, personal, confidential, and regulated information. It sets forth guidelines for data discovery, classification, and mapping to understand data assets' location, sensitivity, and ownership. The chapter defines procedures for maintaining an accurate and up-to-date data inventory, including retention periods, sharing agreements, and disposal practices. It also outlines the responsibilities of individuals involved in data inventory processes, including data owners, IT administrators, and data stewards. Compliance with this policy is mandatory for all individuals within the Company, and any deviations or exceptions require approval from the designated authority responsible for data inventory and cybersecurity governance.
- 4.3. To achieve the Company's overall mission, and the purpose of this cybersecurity policy, the Company shall:
- DTA-01 Maintain a data inventory management system to track data managed by the Company.
 - DTA-02 Ensure the Company's data inventory management system maintains an Inventory of data managed by the Company and under its control.
 - DTA-03 Ensure the Company's data inventory management system maintains an Inventory of data managed by the Company and under the control of third parties.



- DTA-04 Ensure the Company's data inventory management system maintains documented definitions of categories of data managed by the Company.
- DTA-05 Ensure the Company's data inventory management system defines data owners for all data managed by the Company.
- DTA-06 Ensure the Company's data inventory management system tracks the necessity of the data managed by the Company when the Company's data owners approve it.
- DTA-07 Ensure the Company's data inventory management system tracks the business purpose of all data managed by the Company.
- DTA-08 Ensure the Company's data inventory management system tracks data that should be masked in information systems.
- DTA-09 Ensure the Company's data inventory management system tracks the classification, criticality, and sensitivity of all data managed by the Company.
- DTA-10 Ensure the Company's data inventory management system documents the location of all data managed during the processing lifecycle.
- DTA-11 Maintain a system to automatically inventory and classify items managed by the Company (whether onsite or located at a third party).
- DTA-12 Ensure that the Company's data inventory system automatically discovers data managed by the Company (whether onsite or at a third party).
- DTA-13 Ensure that the Company's data inventory system automatically classifies and labels data managed by the Company (whether onsite or located at a third party).
- DTA-14 Ensure that the Company's data inventory system automatically discovers when its private data is located in publicly available locations.
- DTA-15 Ensure that the Company's data inventory system is integrated with the Company's asset inventory system.
- DTA-16 Ensure that the Company's data inventory system logs and alerts events related to the data managed by the Company (such as access, changes, and deletions).
- DTA-17 Ensure that the Company's data inventory system logs and alerts events related to the system configuration files managed by the Company (such as access, changes, and deletions).
- DTA-18 Define a process the Company shall use to define data retention periods for different types of data managed by the Company.
- DTA-19 Define a process the Company shall use to archive data managed by the Company whenever possible.



5. Database Credentials Standard

- 5.1. This chapter states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of the Company's networks. Software applications running on the Company's networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.
- 5.2. This chapter is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the Company network. This policy applies to all software (programs, modules, libraries or APIs that will access a Company, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitized information.
- 5.3. In order to maintain the security of Company's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text or easily reversible encryption. Database credentials must not be stored in a location that can be accessed through a web server. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
- 5.4. Storage of Data Base Usernames and Passwords:
- Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
 - Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
 - Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
 - Database credentials may not reside in the documents tree of a web server.
- 5.5. Retrieval of Database User Names and Passwords:
- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use.



Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

5.6. Access to Database Usernames and Passwords:

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Developer groups must have a process in place to ensure that database passwords are controlled. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.
- Users and/or software accessing sensitive data must be subjected to proper access control and should not be able to perform privileged operations that are out of scope of said user and/or software.

6. Cloud Service Provider Management

6.1. Our Cloud Service Provider Management policy is designed to establish a comprehensive and systematic framework for the selection, engagement, and continuous oversight of cloud services within our Company. This chapter delineates clear criteria and protocols for evaluating potential cloud service providers, ensuring that they meet our stringent security, privacy, and operational performance standards. By laying out structured due diligence and risk assessment procedures, this chapter is instrumental in mitigating the potential risks associated with cloud computing, such as data breaches, service disruptions, and compliance lapses.

6.2. The Cloud Service Provider Management policy applies to all personnel within our Company, including full-time employees, part-time staff, consultants, and external business partners who interact with cloud computing resources. This policy comprehensively encompasses cloud service providers' selection, implementation, and management. It delineates the scope of cloud services across our infrastructure, including but not limited to SaaS, PaaS, and IaaS models. It prescribes the standards for evaluating potential providers' security posture, managing cloud access controls and data protection mechanisms, and integrating cloud services with our existing IT environment. The policy mandates consistent and rigorous assessments to ensure that cloud engagements align with our Company security requirements, data governance policies, and



regulatory compliance mandates. Adherence to this policy is compulsory for all applicable entities within the company, and it necessitates that any exemptions or deviations be formally reviewed and sanctioned by the appointed governance body overseeing cloud strategy and cybersecurity directives.

6.3. To achieve the Company's overall mission, and the purpose of this cybersecurity policy, the Company shall:

- CSP-01 Maintain an inventory of each of the Company's authorized Cloud Service Providers (CSPs).
- CSP-02 Maintain an inventory of each service authorized for use in each authorized Cloud Service Provider (CSP).
- CSP-03 Maintain an inventory of the Company's authorized Software-as-a-Service (SaaS) providers.
- CSP-04 Maintain an inventory of the accounts authorized for use in each of the authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers.
- CSP-05 Maintain a cybersecurity configuration benchmark for each of the Company's authorized Cloud Service Providers (CSPs).
- CSP-06 Maintain a cybersecurity configuration benchmark for each of the services authorized for use in each of the Company's authorized Cloud Service Providers (CSPs).
- CSP-07 Maintain a cybersecurity configuration benchmark for each of the Company's authorized Software-as-a-Service (SaaS) providers.
- CSP-08 Maintain a cloud configuration vulnerability management system to regularly scan each of the Company's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers for potential cybersecurity vulnerabilities.
- CSP-09 Maintain a Data Loss Prevention (DLP) system to log and alert on potential data loss events in the Company's Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers regularly.
- CSP-10 Ensure that appropriate logs from the Company's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are enabled on the cloud platform.
- CSP-11 Ensure that appropriate logs from the Company's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are aggregated into the Company's log management system.

7. Artificial Intelligence Standard

7.1. The Company is committed to full compliance with applicable laws related to the use of artificial intelligence in the countries in which the Company provides products and services. Additionally, the Company is committed to the ethical use of artificial intelligence. This chapter outlines the Company's requirements with respect to the adoption of all forms of artificial intelligence at the Company. Such



artificial intelligence adoption includes use for business efficiencies, operations, and inclusion in the Company's products and services.

7.2. This chapter is applicable to all Company directors, officers, board members, employees, contractors, representatives, affiliates, agents, and any person or entity performing services for or on behalf of the Company.

7.3. Definitions:

- "Artificial intelligence" or "AI" means the use of machine learning technology, software, automation, and algorithms to perform tasks and make rules or predictions based on existing datasets and instructions.
- "Artificial Intelligence Committee" or "AI Committee" is an internal Company committee tasked with reviewing and approving uses of AI at the Company.
- "Artificial intelligence system" or "AI system" means software that is developed with one or more of the techniques and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.
- "Closed AI system" means an AI system where the input provided by one user is used to train the AI model. Input data from the user is isolated from other users, and the data is considered more secure.
- "Embedded AI Tools" means AI tools embedded in existing software tools approved and used at the Company and which do not require approval for use from the AI Committee.
- "Government" means the government of a country or subdivision thereof.
- "Government Entity" means any entity controlled by a government in whole or part. This includes Government-owned or controlled (whether whole or partial ownership or control) commercial enterprises, institutions, agencies, departments, instrumentalities, and other public entities, including research institutions and universities.
- "Government Official" means any officer or employee of a Government Entity, an official of a political party, a candidate for political office, officers and employees of non-governmental international organizations, and any person with responsibility to allocate or influence expenditures of Government funds. This includes data scientists and researchers who are employed by a government or a Government Entity. Employees at government organizations are considered Government Officials regardless of title or position.
- "Non-public Company data" means any information that, if disclosed, could violate the privacy of individuals, government regulations or statutes, could jeopardize the financial state of the Company, could injure its reputation, or could reduce its competitive advantage.



- “Open AI system” means an AI system where the input provided by all users is used to train the AI model. Input data from all users is not private and may be revealed to other users.
- “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household.

7.4. Guiding Principles:

- 7.4.1. The intent of this Policy is to provide general guidance on the use of AI at the Company so that the Company can leverage the use of AI as a tool while ensuring it continues to meet legal obligations and act in an ethical manner. The use of AI at the Company should never compromise the Company’s core values or introduce undue risk to the organization. Rather, the use of AI at the Company should be focused on improving business efficiencies and enhancing the Company’s ability to fulfill its mission.
- 7.4.2. It is important to remember that the Company is a global organization. The Company has entities and staff globally and provides its products and services to customers globally as well. Accordingly, this chapter provides overarching guidance based on global standards for the use of AI.
- 7.4.3. This policy is not intended to address every use of AI at the Company. There are certain business departments and functions at the Company that bear more considerations and potential risks. Before using any AI at the Company — whether for personal business tasks such as writing an email or more complex business processes such as analyzing datasets - you should consult with your manager and seek guidance. Also, please see Prohibited Uses below for situations in which AI may not be used at the Company, and High-Risk Use of AI systems for situations in which extreme caution is required when considering using AI.
- 7.4.4. In addition, there are certain Embedded AI Tools used in existing approved Company software that do not require additional approval for use. For example, the use of Microsoft Word in which Microsoft Word has embedded an AI tool to check spelling or grammar. The use of Embedded AI Tools in approved software at the Company is permitted, provided those software tools are aligned with previous general business uses.
- 7.4.5. When third-party software, services, or contractors are utilized or employed, any AI usage by software used by these parties or services must be noted and evaluated carefully. Contracted services that utilize AI technology should be considered in the same light as individual AI usage. Consult with



the Legal Department about the inclusion of an AI-specific clause in any vendor or contractor agreements.

7.4.6. The following principles must be followed when considering using an AI system at the Company:

- The use of an AI system should primarily focus on completing departmental goals as directed by company leadership. Except for the use of an Embedded AI Tool in a software system approved for use at the Company, any use of a new AI System at the Company must be approved by the AI Committee.
- Individuals using an AI system must have expertise in the subject matter for which the AI is used. AI is to be utilized as a tool and is not a substitute for expertise. For example, if using AI for coding, the individual deploying the AI must have expertise in coding.
- All AI-generated content (writing, datasets, graphs, pictures, etc.) must be thoroughly reviewed by an individual with expertise to evaluate such content for accuracy as well as general proofing and editing. AI-generated content should be viewed as a starting point, not the finished product. Like any content at the Company, AI-generated content should conform to the look and feel of the Company brand and voice.
- Any use of an AI system must have clear objectives for the AI use as a tool and business-accepted data sets from which the AI draws. If the data sets that the AI is using are not accurate, then the information AI provides will not be accurate.
- AI systems are trained on data that may contain inherent bias. Users of these systems are responsible for reviewing any AI-produced content for bias and correcting it as necessary.
- Non-public Company information must never be put into an open AI system.
- The use of an AI system must be documented to capture institutional knowledge. For example, if AI is used to create code and included in a larger section of code, there must be documentation as to which code section is AI-derived and who reviewed it.
- The use of an AI system must meet any terms of use or contractual limitations. Contractual restrictions or terms of use may restrict the Company's use of an AI system that would otherwise be legally compliant and ethically sound. For example, an AI system's terms of use may require the use of certain disclaimers in certain use situations or prohibit the use of the AI system to do certain tasks. The Company should have all terms of use or contracts for AI systems reviewed by the Legal Department to ensure compliance with contractual obligations in using an AI system.



- 7.5. Prohibited Uses. There are certain uses of AI that are prohibited. Unless otherwise approved by the AI Committee and respective department heads, you are prohibited from using AI systems for any of the following activities at any time:
- Conducting political lobbying activities is prohibited. Lobbying is defined as any action aimed at influencing a Government, Government Official, or Government Entity for any reason.
 - Using AI systems to identify or categorize candidates, employees, contractors, or other affiliated entities based on protected class status is prohibited.
 - Entering trade secrets, confidential information, or personal data about any individual into an open AI system.
 - Using an AI system to obtain legal advice, including, but not limited to, creating policies for internal use or to provide to third parties.
 - Creating intellectual property that the Company desires to register and/or holds significant value to the Company.
- 7.6. Ethical Guidelines. The Company desires to act in an ethical manner when using AI. Accordingly, there may be uses of AI that are legally permissible but which do not meet ethical requirements. Any use of an AI system at the Company should conform to the following ethical guidelines:
- Informed Consent: Prior to inputting personal information into a closed AI system, ensure that you have obtained informed consent from the individual(s) whose personal information will be inputted.
 - Integrity in Use: All users of AI systems should be honest about how AI helped in getting the work done. Even if using an AI system approved by the AI Committee for an approved use, you should ensure your manager or the department requesting a task for which you are using an AI system is aware of your use of the AI system. Do not pass off AI-generated work as done by you solely. Additionally, you should ask permission if you desire to use an AI system tool to complete a task. For example, you should ask your manager and HR representative if you may use an AI system to assist in writing a performance evaluation.
 - Appropriate Content: Do not use company time or resources to generate content using an AI system that would be considered illegal, inappropriate, harmful to the Company's brand or reputation, or disrespectful to others.
 - Unauthorized Use: Do not use Company time or resources to generate content using an AI system for personal use without prior approval of the appropriate department leader.
- 7.7. High-Risk Use of AI Systems. There are certain uses of AI systems that are more high risk than others. As a global company, we are committed to complying with all AI legal requirements and guidance in the countries in which we operate. The European Union ("EU") has classified the following potential uses of AI as posing a high risk to the health and safety or fundamental rights of natural persons.



Therefore, there are several additional requirements for the use of AI systems in such cases:

- **Personal Data in AI Systems:** AI should be used with extreme caution when inputting any personal data of an individual into a closed AI system (it is prohibited to put any personal data into an open AI system).
- **Screening Job Candidates:** AI should be used with caution when screening any job applicants to ensure it does not adversely impact protected class members or introduce any bias. Equity and inclusion issues surrounding AI use in job screening are a potential source of litigation.
- **Personnel Decisions:** AI should be used with caution for any use related to making decisions on promotions, retention, or similar personnel such decisions. Extreme caution should be utilized to ensure that biases (including biases found in existing data sets) are avoided.

8. Data Breach Notification and Incident Response Plan

8.1. We take data security seriously. In the event of a personal data breach that may pose a risk to the rights and freedoms of our users, we follow a clear incident response procedure in accordance with the General Data Protection Regulation.

8.2. Our actions in the event of a data breach include:

8.2.1. **Detection and Containment:** Immediate identification of the breach and containment of its impact using technical and organizational measures. All relevant systems and access points are reviewed to prevent further compromise.

8.2.2. **Internal Notification and Assessment:** The incident is escalated to our Information Security team and senior management. The nature, scope, and potential consequences of the breach are evaluated within **24 hours** of discovery.

8.2.3. **Notification to Supervisory Authority:** If the breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the competent data protection authority **without undue delay and, where feasible, within 72 hours** after becoming aware of the breach.

8.2.4. **Notification to Affected Users:** Where the breach is likely to result in a high risk to the rights and freedoms of affected individuals, we will also inform them **without undue delay**, in clear and plain language, about:

- the nature of the breach;
- the likely consequences;
- the measures taken or proposed to be taken;
- contact details of our DPO for further information.

8.2.5. **Documentation and Post-Incident Review:** All data breaches, regardless of severity, are documented internally, including facts relating to the breach, its effects, and the remedial actions taken. A root cause analysis is



conducted, and additional safeguards are implemented where necessary to prevent recurrence.

- 8.3. If you suspect a security issue related to your personal data or identify a potential breach, please report it immediately by contacting us at e-mail.

9. Sanctions

- 9.1. Non-compliance with this policy may result in disciplinary action in line with our Company's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.



22-05-2026
Ecorpp Management N.V.
Boy Hendriks

