

CORPORATE INFORMATION SECURITY POLICY

NETGAME ENTERTAINMENT N.V.

TABLE OF CONTENTS

1.1. Purpose	4
1.2. Scope	4
1.3. History	4
1.4. Responsibilities	5
1.5. General Policy Definitions	6
1.6. Regulatory Compliance	6
2. IT Asset Policy	7
2.1. Purpose	7
2.2. Scope	7
2.3. Policy Definitions	7
3. ACCESS CONTROL POLICY	9
3.1. Purpose	9
3.2. Scope	9
3.3. Policy Definitions	9
4. PASSWORD CONTROL POLICY	13
4.1. Purpose	13
4.2. Scope	13
4.3. Policy Definitions	13
5. EMAIL POLICY	17
5.1. Purpose	17
5.2. Scope	17
5.3. Policy Definitions	18
6. INTERNET POLICY	19
6.1. Purpose	19
6.2. Scope	19
6.3. Policy Definitions	20
7. ANTIVIRUS POLICY	20
7.1. Purpose	20
7.2. Scope	20
7.3. Policy Definitions	20
8. INFORMATION CLASSIFICATION POLICY	21
8.1. Purpose	21
8.2. Scope	21

Corporate Information Security Policy – NetGame Entertainment N.V.

8.3. Policy Definitions	21
9. REMOTE ACCESS POLICY	25
9.1. Purpose	25
9.2. Scope	25
9.3. Policy Definitions	25
10. OUTSOURCING POLICY	26
10.1. Purpose	26
10.2. Scope	26
10.3. Policy Definitions	26
11. ANNEX	26
11.1. Glossary	26

INTRODUCTION

This document specifies the level of security as well as the approach that must be established and applied across NetGame Entertainment N.V. for the safeguarding of data and information against threats.

1.1. Purpose

This Security Policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in the Organization. Its goal is to protect the Organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

NetGame Entertainment N.V. (hereafter referred to as “Organization”) seeks to ensure that the confidentiality, integrity and availability of all the information in its custody, be it internal or player information, is maintained by implementing best practices and policies to minimise risk.

The data stored in electronic systems used by NetGame Entertainment N.V. represents an extremely valuable asset. The focus and mode of operation of NetGame Entertainment N.V. as an online gaming company and its reliance on information technology for the delivery of its services makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion. The need to transmit this information across different networks of computers renders the data more vulnerable to accidental or deliberate unauthorised modification or disclosure.

The purpose of this Information Security Policy is to preserve an appropriate level of:

- **Confidentiality:** the prevention of the unauthorised disclosure of information
- **Integrity:** prevention of the unauthorised amendment or deletion of information
- **Availability:** prevention of the unauthorised withholding of information or resources

1.2. Scope

This document applies to all the users and employees in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document and other related referenced documents is mandatory for this constituency. This policy applies to all data, systems and networks owned or operated by NetGame Entertainment N.V.

1.3. History

Version	Description	From	Author
1.0	Initial version	9 th June 2019	CTO

Corporate Information Security Policy – NetGame Entertainment N.V.

2.0	Revised version	31 st August 2020	CTO
3.0	Revised version	20 th November 2025	CTO
4.0	Revised version	20 th July 2026	CTO

1.4. Responsibilities

Role	Responsibilities
Chief Executive Officer	☐ Overall direction towards information security and cyber-resilience.
Chief Information Officer	☐ Accountable for all aspects of the Organization's information security.
Key Official/Director	☐ Responsible for ensuring that the gaming system is consistently and continuously in line with regulations and license conditions, including security
Information Security Office	☐ Responsible for the security of the IT infrastructure. ☐ Plan against security threats, vulnerabilities, and risks. ☐ Implement and maintain Security Policy documents. ☐ Ensure security training programs. ☐ Ensure IT infrastructure supports Security Policies. ☐ Respond to information security incidents including notification to authorities where applicable ☐ Help in disaster recovery plans.
Information Owners	☐ Help with the security requirements for their specific area. ☐ Determine the privileges and access rights to the resources within their areas.
IT Security Team	☐ Implements and operates IT security. ☐ Implements the privileges and access rights to the resources. ☐ Supports Security Policies.
Users	☐ Meet Security Policies. ☐ Report any attempted security breaches.
Entire Organization constituency	☐ Adhere to the Corporate Information Security Policy and related documents

	☐ Report unusual behavior or malicious activity to the IT Security Team
--	--

1.5. General Policy Definitions

1. Exceptions to the policies defined in any part of this document may only be authorized by the Information Security Office. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
2. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed.
3. All the IT services should be used in compliance with the technical and security requirements defined in this and other referenced documents.
4. Infractions of the policies in this document may lead to disciplinary actions. In some serious cases they could even led to prosecution and/or dismissal.

1.6. Regulatory Compliance

1. NetGame Entertainment N.V. shall comply with all applicable laws, regulations, and guidelines issued by the Curaçao Gaming Authority (CGA) and any other relevant supervisory bodies. All information security controls and operational processes shall align with current CGA requirements and recognized industry best practices.
2. The Organization shall ensure the ongoing integrity and security of its technical environment through periodic security testing, which may include vulnerability assessments, penetration testing, and other evaluations as required by applicable regulations. Additional testing shall be performed following any significant system changes.
3. NetGame Entertainment N.V. shall maintain internal processes for documenting, reviewing, and escalating security incidents and audit findings. Information related to material incidents or audit outcomes shall be made available to the CGA upon request and reported within applicable timelines.
4. The Organization shall apply appropriate safeguards to protect personal and sensitive information, including the use of industry-standard encryption and secure storage methods. Data shall be retained for a minimum of five (5) years or for a longer period if required by applicable regulations.
5. NetGame Entertainment N.V. shall ensure that system updates, new releases, and operational changes are reviewed for security impact. No update or change shall be moved into production unless required security controls have been validated as effective.
6. The Organization aligns its information security controls with the CGA Information Security Control Requirements for CGA Licensees (B2C and B2B) and adopts the Center for Internet

Security (CIS) Controls Implementation Group 1 (IG1) as its mandatory baseline, to be implemented within twelve (12) months of licence issuance or publication of those requirements, with Implementation Group 2 (IG2) as a strategic target within 24 to 36 months. As a B2B gaming technology provider, NetGame Entertainment N.V. is subject to these requirements in its own right as a CGA licensee.

7. The Organization notifies the CGA without undue delay, and in any event within twenty-four (24) hours, of any security incident that compromises gaming integrity, affects player funds or personal data, or may impact regulatory reporting, system availability, or game fairness, in accordance with Article 5 of the LOK and the applicable CGA licence conditions. Failure to notify constitutes a breach of licence conditions.
8. As the supplier of certified Remote Gaming Servers, game engines, RNG, and game content, the Organization is directly responsible for obtaining, maintaining, and renewing all required certifications for its gaming components, and proactively notifies its B2C operator clients and the CGA of any change to certification status, including lapses, withdrawals, scope changes, or pending renewals.
9. The Organization demonstrates compliance through annual self-assessment reports using CGA-provided templates and through independent third-party security audits, and provides the CGA with the reports required under its licence conditions, including a change report, an incident report, and a report by an independent expert approved by the CGA, within the timeframes specified by the CGA.

2. IT ASSET POLICY

2.1. Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in the Organization.

2.2. Scope

The IT Assets Policy is aimed at anyone, including NetGame Entertainment N.V. employees, users, temporary workers, visitors, partners and suppliers, using desktops, laptops, printers, applications and software, involved in the provision of IT services.

2.3. Policy Definitions

1. IT assets must only be used in connection with the business activities they are assigned and / or authorized.
2. All the IT assets must be classified into one of the categories in the Organization's security categories; according to the current business function they are assigned to.

3. Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
4. All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.
5. Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.
6. Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.
7. All personnel interacting with the IT assets must have the proper training.
8. Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
9. Access to assets in the Organization location must be restricted and properly authorized, including those accessing remotely. Company's laptops, PDAs and other equipment used at external location must be periodically checked and maintained.
10. All IT assets supporting the gaming system shall have their clocks synchronized with a single, reliable time source. Configuration of date or time on any such component shall be technically restricted only permissible to NetGame Entertainment N.V. IT Security based on formal written approvals and subject to Change Management. All date and time related operations (including attempts to amend) shall be recorded in an audit trail whose logs are shipped to NetGame Entertainment N.V. IT Security
11. The IT Technical Teams are the sole responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
12. Special care must be taken for protecting laptops, PDAs and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields and falls.
13. When travelling by plane, portable equipment like laptops and PDAs must remain in possession of the user as hand luggage.
14. Disk encryption and erasing technologies should be considered and implemented where possible in portable assets in case they were stolen
15. Operating system firewalls should be enabled and managed
16. Where applicable, IT assets shall be running supported operating systems and builds
17. IT assets within defined scopes shall undergo a periodical vulnerability assessment as well as penetration testing in order to address any weaknesses
18. Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the Information Security Office.
19. Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an Information Security Team member. Assets storing

sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

3. ACCESS CONTROL POLICY

3.1. Purpose

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in the Organization.

3.2. Scope

The Access Control Policy is aimed at anyone, including NetGame Entertainment N.V. employees, users, temporary workers, visitors, partners and suppliers with limited or unlimited access time to services.

3.3. Policy Definitions

1. A data owner shall be formally identified and designated for every given service supporting NetGame Entertainment N.V. operations. The data owner shall approve (or otherwise) all requests for access to the respective system. No access shall be granted to a service/system/data without the formal approval of the respective designated data owner. The data owner shall be responsible to trigger periodical (consistent) reviews of access and update where and if necessary.
2. The data owner shall ensure that one single updated procedure is in place for adherence to by the technical people who shall interact with the system for the purpose of managing approved access transactions. All requests for access shall only be channeled through one single company-wide ticketing system. No other channels (such as email or instant messaging) are authorized for the submission of access requests. No access beyond the approved access shall be granted
3. Unless not technically possible, all systems shall make use of a centralized authentication mechanism such as directory services. All information repositories (including and not limited to servers, application, networks, storage, cloud, etc) shall require authentication for access. There shall be no such repository accessible without formal authentication
4. The data owner has the authority and accountability to review access in case of tangible suspicion of wrongdoing or malicious intent
5. Any system that handles valuable information must be protected with a password-based access control system.
6. Any system that handles confidential or sensitive information must be protected and isolated by a two factor -based access control system as well as a different network segment (with only the required network ports open on the firewalls)
7. Components connected to the network producing suspicious behavior may be disconnected without notice by IT Security

8. Discretionary access control list must be in place to control the access to resources for different groups of users.
9. Access to resources should be granted on a per-group basis rather than on a per-user basis.
10. Access shall be granted under the principle of “least privilege”, i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions.
11. Whenever possible, access should be granted to centrally defined and centrally managed identities.
12. Employees are prohibited from tampering or evading access control in order to gain greater access than they are assigned. Use of programs and applications with aim of doing so is strictly prohibited. Installation of such applications may be monitored through central functions such as a Network Operations Centre or a Security Operations Centre
13. Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.
14. Employee accounts inactive for a period of 3 (three) months shall be disabled and only activated following a formal request approved by the respective data owner
15. Use of generic usernames shall be kept to a minimum only for scenarios approved by IT Security. For all other instances all stakeholders shall be provided with a unique, standard, identifiable username
16. All authenticated sessions shall be restricted to office hours access. Different requirements shall be approved by the respective data owner
17. Periods of authenticated inactivity shall be disconnected or (where applicable) protected with end point locking. Such period is 5 (five) minutes.
18. All system authentications (and attempts) are logged and shipped to a Security Information and Event Management (SIEM) system. This includes authentication by authority representatives, audits and other parties
19. All networks, by function, shall be segregated using VLANs or other technologies. Access lists between networks shall be logged and any amendments is subject to a logged approved request
20. The below statements are also applicable:
21. New Users (Joiners)

The new resource's manager is responsible to request access for the new employee/s. The request for access shall be approved by the Information Security Office, the Key Official and the respective service owner as a minimum. If access is approved by all stakeholders, it is then granted by the system administrator holding the privileged rights. The resource's manager is bound to maintain a list of granted access requests in line with requirements and policies (including data protection).

Request for access change of existing users

Should any changes to the existing user privileges be required, the resource's manager shall log a service request for approval from the Information Security Office, Key Official and the respective service owner. Reasons for the changes should always be included in the request especially when an additional access level is being granted. The list of granted access requests shall be updated by the resource's manager.

User Termination (Leavers)

Terminated or terminating resource's Managers shall be responsible to initiate the request for termination by logging a service request in balance with the applicable notice period of the particular employee/s. The user should be disabled on the last day of employment where any access to the system should be revoked. The Key Official shall ensure that details of previously held access should be retained as needed ensuring that retention is in line with the requirements in the General Data Protection Regulation (GDPR).

22. Access Distribution

This section includes more details about the type of access per job roles.

Existing Job roles

Administration

- ☐ Directors and Key Official
- ☐ Management and Finance
- ☐ Client Account Managers

Technical

- ☐ Systems Development and Application Support
- ☐ Network and Systems Support

Access Distribution

Administration

Directors and Key Official have the right to request access and information to any part of the system. All requests shall be logged. Access for Client Account Managers needs to be approved according to need and also be logged.

Technical

The below table describes the access type typically granted per technical group:

Job Designation	Access to Source Control	Remote Access (VPN)	Physical Access	Database Access	Network Management Access	Application Server Access
☐ System Development ☐ Application Support	Granted	Granted	Not Granted	Granted	Not Granted	Granted
☐ Network ☐ Systems Support	Not Granted	Granted	Granted	Not Granted	Granted	Granted

Job Designation	Access to Management Site	Physical Access	Application Server Access
☐ Site and Game Management	Granted	Not Granted	Not Granted

23. Remote Access and teleworking

In order to ensure adequate security NetGame Entertainment N.V. only allows network access to equipment management and servers whilst connected via VPN. Access to site management is secured over an https connection and via user and password authentication. Any remote access requests should be approved by the key official. All teleworking shall be formally approved at the discretion of the respective manager or Human Resources. For teleworking, the employee shall:

- ☐ Refrain from working from public places such as pubs, restaurants, etc
- ☐ Ensure they are not subject to shoulder surfing (including having displays towards and within range of CCTV cameras)
- ☐ Always connect via VPN
- ☐ Adhere to all NetGame Entertainment N.V. policies at all times
- ☐ Not disclose any information to by-standers, including to relatives and/or acquaintances

24. Physical Access

Physical access to NetGame Entertainment N.V. and related data centres must be strictly controlled. Control will be enforced via access authorization issued by the Key Official or delegated authority. All physical access to the servers will be logged and filed for future auditing and reporting purposes. This includes all changes to the physical setup such as equipment addition and removal.

25. Third Party Access

Third Parties are not allowed to access the data centre where NetGame Entertainment N.V. services are hosted unless accompanied at all times by an authorized individual appointed by the key official. Third party visits shall be logged including visitor signature, full name, reason and duration.

4. PASSWORD CONTROL POLICY

4.1. Purpose

The Password Control Policy section defines the requirements for the proper and secure handling of passwords in the Organization.

4.2. Scope

This policy applies is aimed at anyone, including NetGame Entertainment N.V. employees, users, temporary workers, visitors, partners and suppliers with limited or unlimited access time to services.

4.3. Policy Definitions

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

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Every user must have a separate, private identity for accessing IT network services.
3. Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
4. Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be at least 8 characters long.
5. Each regular user may use the same password for no more than 90 days and no less than 3 days. The same password may not be used again for at least one year.
6. Password for some special identities will not expire. In those cases, password must be at least 15 characters long and subject to Key Official or delegate approval.
7. All privileged account passwords across all assets (e.g., root, local/domain administrator, application administration accounts, etc.) must be changed on at least every three months. This includes any SNMP community strings. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
8. All out-of-the box default passwords shall be changed in line with this policy before deployment of the artefact into any environment (staging, testing, or live)
9. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
10. Passwords must not be inserted into email messages or other forms of electronic communication.
11. Use of administrative credentials for non-administrative work is not permitted. IT administrators must have two set of credentials: one for administrative work and the other for non-privileged work.
12. Sharing of passwords is forbidden. Passwords should not be revealed or exposed to public sight.
13. Whenever a password is deemed compromised, it must be changed immediately and a ticket assigned to Information Security Office is logged.
14. For critical applications, digital certificates and multiple factor authentication using smart cards should be used whenever possible.
15. Identities must be locked if password guessing is suspected on the account.
16. Guidelines:

General Password Construction Guidelines

Passwords are used for various purposes within the company. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail

password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- ❑ The password contains less than fifteen characters
- ❑ The password is a word found in a dictionary (English or foreign)
- ❑ The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words referring to the company name or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxxvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, lsecret)

Strong passwords have the following characteristics:

- ❑ Contain both upper and lower case characters (e.g., a-z, A-Z)
- ❑ Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&"()_+1--
- ❑ Are at least fifteen alphanumeric characters long and is a passphrase (Ohmylstubbedmyt0e).
- ❑ Are not a word in any language, slang, dialect, jargon, etc.
- ❑ Are not based on personal information, names of family, etc.
- ❑ Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmBlw2R!" or "Tmb1W>r-" or some other variation.

NOTE: Do not use any of the examples in this document as passwords!

Password Protection Standards

Do not use the same password for company accounts as for other non- company-access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various company access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share the company's passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential company information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them seek prior written approval from the Key Official or the the Information Security Department. Report any suspicious or malicious activity.

Do not use the "Remember Password" feature of applications.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system unless an authorized secure password vault is implemented across the organization.

Change passwords at least once every three months (including system-level passwords).

If an account or password is suspected to have been compromised, report the incident and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the company or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

Application developers must ensure their programs contain the following security precautions.

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Use of Passwords and Passphrases for Remote Access Users

Access to the company networks via remote access is to be controlled using either a one- time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe-I 0-1W as*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5. EMAIL POLICY

5.1. Purpose

The Email Policy section defines the requirements for the proper and secure use of electronic mail in the Organization.

5.2. Scope

This policy applies is aimed at anyone, including NetGame Entertainment N.V. employees, users, temporary workers, visitors, partners and suppliers with limited or unlimited access time to NetGame Entertainment N.V. email services.

5.3. Policy Definitions

1. All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the Organization. Occasional use of personal email address on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in the Organization system resources and the productivity of the work is not affected.
2. Use of the Organization resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the Organization business is strictly forbidden.
3. In no way may the email resources be used to reveal confidential or sensitive information from the Organization outside the authorized recipients for this information.
4. Using the email resources of the Organization for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is forbidden.
5. Use of the Organization email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
6. Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriated.
7. Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged. However, only the Information Security Office may approve the interception and disclosure of messages.
8. Identities for accessing corporate email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the company's procedures for managing identities. Sharing of passwords is discouraged. Users should not impersonate another user.
9. Outbound messages from corporate users should have approved signatures at the foot of the message.
10. Attachments must be limited in size according to the specific procedures of the Organization. Whenever possible, restrictions should be automatically enforced.
11. Whenever possible, the use of Digital Rights technologies is encouraged for the protection of contents.
12. Scanning technologies for virus and malware must be in place on endpoints and servers to ensure the maximum protection in the ingoing and outgoing email.

13. Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.
14. Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT Continuity Management.
15. Specifically, the following activities are strictly prohibited, with no exception:
 - ☐ Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
 - ☐ Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
 - ☐ Unauthorized use, or forging, of email header or signature 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).
 - ☐ The company email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any company employee should report the matter to their supervisor immediately.
 - ☐ Using a reasonable amount of company resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a company email account is prohibited. Virus or other malware warnings and mass mailings from the company shall be approved by the VP Operations before sending. These restrictions also apply to the forwarding of mail received by a company employee

6. INTERNET POLICY

6.1. Purpose

The Internet Policy section defines the requirements for the proper and secure access to Internet.

6.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

6.3. Policy Definitions

1. Limited access to Internet is permitted for all users.
2. The use of Messenger service is permitted for business purposes.
3. Access to pornographic sites, hacking sites, and other risky sites is forbidden.
4. No software shall be downloaded without prior approval from Information Security or delegate. Pre-defined procedures shall be in place for this purpose.
5. Internet access is mainly for business purpose. –some limited personal navigation is permitted if in doing so there is no perceptible consumption of the Organization system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
6. Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.
7. In accessing Internet, users must behave in a way compatible with the prestige of the Organization. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
8. Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the Information Security Office.
9. Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

7. ANTIVIRUS POLICY

7.1. Purpose

The Antivirus Policy determines the direction for antivirus together with other forms of protection at NetGame Entertainment N.V.

7.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. It also applies to servers and other equipment as applicable.

7.3. Policy Definitions

Only corporate standard and NetGame Entertainment N.V.-supported anti-virus software should be used and this must be kept up to date to be effective. Files or macros attached to an email sent from an unknown sender should not be opened; such attachments are usually malicious and so should be deleted immediately. Files should never be downloaded from unknown or suspicious sources. Direct disk sharing with read/write access should be avoided unless there is absolutely a business requirement to do so. New viruses are discovered almost every day so the user should never intentionally stop the antivirus software from updating. The below statements also apply and direct further:

1. All computers and devices with access to the Organization network must have an antivirus client installed, with real-time protection.
2. All servers and workstations owned by the Organization or permanently in use in the Organization facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connect to the Organization's network or that can be managed via secure channels through Internet.
3. Organization's devices permanently working in other Organization's network may be exempted from the previous rule if required by the Security Policies of the other Organization, provided those computers will be protected too. Such devices need to be ensured they are malware free before connecting to NetGame Entertainment N.V. network again.
4. Traveling computers from the Organization that seldom connect to the Organization network may have installed an approved antivirus independently managed. This shall be kept to a minimum and only based on the formal approval of the IT Security Team delegate.
5. All the installed antivirus instances must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
6. Visitor computers and all computers that connect to the Organization's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

8. INFORMATION CLASSIFICATION POLICY

8.1. Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the Organization information.

8.2. Scope

This policy applies to all the information created, owned or managed by the Organization, including those stored in electronic or magnetic forms and those printed in paper.

8.3. Policy Definitions

1. Information owners must ensure the security of their information and the systems that support it.
2. IT Security is responsible for ensuring the confidentiality, integrity and availability of the Organization's assets, information, data and IT services.
3. Any breach must be reported immediately to the Information Security Office. If needed, the appropriate countermeasures must be activated to assess and control damages.
4. Information in the Organization is classified according to its security impact. The current categories are defined and detailed below:

All NetGame Entertainment N.V. information is categorized into two main classifications:

- NetGame Entertainment N.V. Public
- NetGame Entertainment N.V. Confidential

NetGame Entertainment N.V. Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to NetGame Entertainment N.V. Systems.

NetGame Entertainment N.V. Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of the Organization. Also included in NetGame Entertainment N.V. Confidential is information that is less critical, such as telephone directories, general corporate information and personnel information amongst others, which does not require as stringent degree of protection.

Corporate Information Security Policy – NetGame Entertainment N.V.

A subset of NetGame Entertainment N.V. Confidential information is "NetGame Entertainment N.V. Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to NetGame Entertainment N.V. by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier/vendor into NetGame Entertainment N.V.'s network to support our operations.

NetGame Entertainment N.V. personnel are encouraged to use common sense judgment in securing NetGame Entertainment N.V. Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact IT Security.

Minimal Sensitivity

General corporate information; some personnel and technical information.

Marking guidelines for information in hardcopy or electronic form:

Note: any of these markings may be used with the additional annotation of "**3rd Party Confidential**".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "NetGame Entertainment N.V. Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "NetGame Entertainment N.V. Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, NetGame Entertainment N.V. information is presumed to be "NetGame Entertainment N.V. Confidential" unless expressly determined to be NetGame Entertainment N.V. Public information by a NetGame Entertainment N.V. employee with authority to do so.

Access: NetGame Entertainment N.V. employees, contractors, people with a business need to know.

Distribution within NetGame Entertainment N.V.: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of NetGame Entertainment N.V. internal mail: Postal mail and other public or private carriers approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it is sent to only approved recipients.

Storage: Keep away from view of unauthorized people; erase whiteboards, do not leave in view on table top. Machines should be administered with security in mind.

Corporate Information Security Policy – NetGame Entertainment N.V.

Protect from loss: electronic information should be backed up on IT Security-approved repositories and have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on NetGame Entertainment N.V. premises; electronic data should be cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

More Sensitive

Business, financial, technical and most personnel information.

Marking guidelines for information in hardcopy or electronic form:

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "**NetGame Entertainment N.V. Confidential**" or "**NetGame Entertainment N.V. Proprietary**", wish to label the information "**NetGame Entertainment N.V. Internal Use Only**" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: NetGame Entertainment N.V. employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within NetGame Entertainment N.V.: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of NetGame Entertainment N.V. internal mail: Sent via Postal mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within NetGame Entertainment N.V., but should be encrypted or sent via a private link to approved recipients outside of NetGame Entertainment N.V. premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on NetGame Entertainment N.V. premises; electronic data should be cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Corporate Information Security Policy – NetGame Entertainment N.V.

Most Sensitive

Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company.

Marking guidelines for information in hardcopy or electronic form:

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that NetGame Entertainment N.V. Confidential information is very sensitive, you may should label the information "**NetGame Entertainment N.V. Internal: Registered and Restricted**", "**NetGame Entertainment N.V. Only**", "**NetGame Entertainment N.V. Confidential**" or similar labels at the discretion of your individual business unit or department. Once again, this type of NetGame Entertainment N.V. Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (NetGame Entertainment N.V. employees and non-employees) designated with approved access and signed non-disclosure agreements.

Automatic Logoff: After period of 30 minutes, user will be logged off from backend system automatically.

Secure Communication: All communication with backend system is done via HTTPS. This is a strict policy where http is not available.

Player Data Security: All player passwords and sensitive information is encrypted with sufficient encryption standards.

Distribution within NetGame Entertainment N.V.: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of NetGame Entertainment N.V. internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: Encrypted distribution within NetGame Entertainment N.V.

Storage: Individual access controls (or RBAC) for electronic information. Physical security including locked repositories and if/where electronically, stored in a physically secured and digitally hardened computer.

Disposal/Destruction: Degaussed, wiped, destroyed.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

9. REMOTE ACCESS POLICY

9.1. Purpose

The Remote Access Policy section defines the requirements for the secure remote access to the Organization's internal resources.

9.2. Scope

This policy applies to the users and devices that need access the Organization's internal resources from remote locations.

9.3. Policy Definitions

1. To gain access to the internal resources from remote locations, users must have the required authorization from IT Security. Remote access for an employee, external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
2. Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates. The software used for remote access, method of authentication and end-to-end process shall strictly abide with the rules issued by IT Security. No attempt to set up remote access shall be carried out based on own initiative.
3. Users must not connect from public computers
4. Connecting to NetGame Entertainment N.V. services while accompanied by 3rd parties (including acquaintances, family or any other) is forbidden

10. OUTSOURCING POLICY

10.1. Purpose

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions and processes.

10.2. Scope

This policy applies to the Organization; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

10.3. Policy Definitions

1. Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
2. Whenever possible, a bidding process should be followed to select between several service providers.
3. In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
4. Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If the

Organization has not enough knowledge and resources, a specialized company should be hired to do the auditing.

5. A service contract and defined service levels must be agreed between the Organization and the service provider.
6. The service provider must get authorization from the Organization if it intends to hire a third party to support the outsourced service, function or process.

11. ANNEX

11.1. Glossary

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An IT service provider that is part of a different organization from its customer.
Identity	A unique name that is used to identify a user, person or role.
Information Security Policy	The policy that governs the organization's approach to information security management
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.

Corporate Information Security Policy – NetGame Entertainment N.V.

ACCEPTANCE

Approved by:

Kostiantyn Kolomiychuk, CTO



Date: 20.07.2026