



WESTWARDWAY
TECH

Information Security POLICY

Introduction

The objective of this information security policy is to foster an environment that will secure information within the Westward Way Tech N. V's infrastructure from threats against privacy, productivity, reputation, or intellectual property rights.

The policy comprehensively applies to all individuals who interact in any way with the company's informational resources in any form.

It details everyone's responsibilities to prevent unauthorised access to physically available information (analogue), and increasingly, electronic information (digital). It is designed to be consistent governmental laws that regulate specific types of information.

Purpose

To safeguard the company's information technology resources and to protect the confidentiality of data, adequate security measures must be taken. This Information Technology Resources Security Policy (hereafter, "Security Policy") reflects the company's commitment to comply with rules and regulations under the Curaçao laws and governing the security of sensitive and confidential information.

Wherever possible, this policy attempts to establish a balance between the risk of loss of information resources, including data misuse, and the effort and cost of the security measures. It includes provisions to reduce, as far as feasible, the risk of theft, fraud, destruction, or other misuses of the company's information technology resources.

Inappropriate exposures of confidential and/or sensitive information, loss of data and inappropriate use of computer networks and systems can be minimised by complying with reasonable standards, attending to the proper design and control of information systems, and applying sanctions when violations of this Security Policy occur.

Security is the responsibility of everyone. It is the responsibility of employees, contractors, software providers and their employees and associates.

All members of staff should become familiar with this Policy's provisions and the importance of adhering to it when using the company's computers, networks, data, and other information resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to:

- Respect the privacy of other users.
- Respect the rights of other users.
- Respect the intended use of resources and systems.
- Respect the integrity of the system or network.
- Adhere to all company policies and procedures.
- Adhere to all applicable regulations and laws.

Scope

This Information Security policy is intended to support the protection, control, and management of the company's information assets. These policies are required to cover all information within the company which could include data and information that is.

- Stored on databases.
- Stored on computers.
- Transmitted across internal and public networks.
- Sent by any communications method.
- Stored on removable media such as CD-ROMs, hard disks, tapes and other similar media.
- Stored on fixed media such as hard disks and disk sub-system.

Objective

To protect the company's business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity, and availability.

To establish safeguards to protect the company's information resources from theft, abuse, misuse, and any form of damage.

To establish responsibility and accountability for Information Security in the company.

To encourage management and staff to maintain an appropriate level of awareness, knowledge, and skill to allow them to minimise the occurrence and severity of Information Security incidents.

To ensure that the company can continue its commercial activities in the event of significant Information Security incidents.

To ensure that the company can comply with all applicable regulations as well as all applicable laws.

Roles & Responsibilities

Roles associated with the Information Security Policy process are defined in the context of the management function and are not intended to correspond with organisational job titles.

Specific roles have been defined according to industry best practises. In some cases, many persons might share a single role; and in other cases, a single person may assume many roles. The significant roles defined for the change management process are:

DIRECTOR OF INFORMATION SECURITY

These roles will all be assigned to our third-party contractor Veracloud.

The Director of Information Security is a senior-level employee of the company who oversees the company's information security program. Responsibilities of the Director of Information Security include the following:

- Developing and implementing a company-wide information security program.

- Documenting and disseminating information security policies and procedures.
- Coordinating the development and implementation of a company-wide information security training and awareness program.
- Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of company Data.
- Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of company Data.

DATA STEWARD

A Data Steward is a senior-level employee of the company who oversees the lifecycle of one or more sets of company Data. Responsibilities of a Data Steward include the following:

- Assigning an appropriate classification to company Data.
- All company Data should be classified based on its sensitivity, value, and criticality to the company.
- Assigning day-to-day administrative and operational responsibilities for company Data to one or more Data Custodians.
- Approving standards and procedures related to day-to-day administrative and operational management of company Data.
- Determining the appropriate criteria for obtaining access to company Data.
- Ensuring that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of company Data.
- Understanding and approving how company Data is stored, processed, and transmitted by the company and by third-party Agents of the company.
- Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity, and availability of company Data.
- Understanding how company Data is governed by company policies, state and federal regulations, contracts, and other legal binding agreements.

DATA CUSTODIAN

A Data Custodian is an employee of the company who has administrative and/or operational responsibility over company Data. In many cases, there will be multiple Data Custodians. A Data Custodian is responsible for the following:

- Understanding and reporting on how company Data is stored, processed and transmitted by the company and by third-party Agents of the company.
- Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of company Data.
- Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of company Data.
- Provisioning and de-provisioning access to company Data as authorised by the Data Steward.
- Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of company Data.

USERS

For the purpose of information security, a User is any employee, contractor or third-party Agent of the company who is authorised to access company Information Systems and/or data. A User is responsible for the following:

- Adhering to policies, guidelines and procedures pertaining to the protection of company data.
- Reporting actual or suspected vulnerabilities in the confidentiality, integrity or availability of company data to a manager or the Information Security Office.
- Reporting actual or suspected breaches in the confidentiality, integrity or availability of company data to the Information Security Office.

Policy

Information security Infrastructure

The information systems are controlled by ensuring that each user accessing the information systems is processed by their job function. This process is described in company's Policy Document "User Management Policy".

Network & Communication Security

The Servers are housed in a certified data centre located at: Veracloud

Network Based (Network IDS)

Network based intrusion detection attempts to identify unauthorised, illicit, and anomalous behaviour based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic.

Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting.

Network Based (Network IDS) Implementation

Network based IDS will monitor traffic and match patterns for malicious activity coming in externally from our network. All external traffic will be monitored and filtered; alerts will be sent to system administrators if there is a serious alarm set off. System administrators will also be responsible for reviewing the minor alerts on a weekly basis.

Host Based (HIDS)

Often referred to as HIDS, host based intrusion detection attempts to identify unauthorised, illicit, and anomalous behaviour on a specific device. HIDS generally involves an agent installed on each system, monitoring and alerting on local OS and application activity as well as agent-less systems whereby either remote access is granted to detect any file configuration changes on network devices such as firewalls and switches, and to monitoring of the syslog server.

The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorised activity. The role of a host IDS is passive, only gathering, identifying, logging, and alerting, but is near-real time monitoring.

Host Based (HIDS) Implementation

The host based intrusion detection will perform file system security checks along with root kit checking. Alongside these two features is a syslog server which can take events from any system which is logging to it and report back any security anomalies that it sees in the logs.

The file integrity checks will ensure that important files within the remote gaming system applications root are not tampered with, as well as ensuring the operating system files integrity – MD5 sums are taken at regular intervals and then re-checked at a later time, if files are changed alerts are sent to the security team.

There is also a real time configuration manager which will notify the system administration team if there are any changes made to any devices, if we see an unauthorised change the security team will immediately carry out an investigation.

Physical (Physical IDS)

Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection is most often seen as physical controls put in place to ensure CIA. In many cases physical intrusion detection systems act as prevention systems as well.

- Examples of Physical intrusion detections are:
- Security Guards
- Security Cameras
- Access Control Systems (Card, Biometric)
- Firewalls
- Man Traps
- Motion Sensors

Intrusion Prevention System (IPS)

Intrusion prevention follows the same process of gathering and identifying data and behaviour, with the added ability to block (prevent) the activity. This can be done with Network, Host, and Physical intrusion detection systems. There are currently no requirements for the IPS as the risk is currently too high in regard to preventing false positives and interrupting service.

System Logs

All network devices and servers log to a secure syslog server. There is proactive monitoring in near real-time that analyses the logs.

OS Patches

All OS patches are tested internally and applied to production on the third day of the month in an exercise named as “Patch day”. Updates are managed and logged via a Windows Update Server.

Workstation Protection

All workstations that access the environment utilise the corporate anti-virus software deployed with every desktop/laptop build.

Windows servers will employ anti-virus software only.

The IDS system will be leveraged for any Linux servers to ensure that no rootkits or Trojans are installed.

Security & System Processes

Every 90 days the following will be tested to ensure that the internal security system is working as designed:

- Testing of accounts of each organisational unit have the correct access rights
- Test all internal servers ensuring that only the required ports are open

Securing Access To The Environment

- Assign a unique identification (ID) to each person with access to ensure that actions taken on critical data and systems are performed by, and can be traced to known and authorised users.
- Identify all users with a unique username before allowing them to access system components.
- In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - System Username/Password
- Implement two-factor authentication for remote access to the network by employees, VPN access with two levels of authentication, SSH username/password and key authentication and Windows username and password.
- Encrypt all passwords during transmission and storage on all system components.
- Ensure proper user authentication and password management for non-consumer users and Administrators on all system components as follows:
 - Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
 - Verify user identity before performing password resets.
 - Set first-time passwords to a unique value for each user and change immediately after the first use
 - Immediately revoke access for any terminated users
 - Remove inactive user accounts at least every 90 days.
 - Enable accounts used by vendors for remote maintenance only during the time period needed.
 - Do not use group, shared, or generic accounts and passwords.
 - Change user passwords at least every 90 days.
 - Require a minimum password length of at least eight characters.
 - 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,
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- Limit SSH access to authorised users, SSH for any application users and root is disabled.
- Limit repeated access attempts by locking out the user ID after not more than six attempts and notify email sent with user account details to begin investigation
- Set the lockout duration to thirty minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

Data Privacy

Personal data processed in testing and development environments

With the intention of being compliant with Data Privacy regulations, development and testing environments must not process personal data that was collected for business motives. In order to process personal data in development and testing environments, the data must be properly obfuscated into a format that cannot be traced back to the respective data subject.

To achieve this type of obfuscation, the following method should be followed:

- Unique attributes such as "first name" and "email" must have one third of the characters altered.
- Credentials must be altered.

Account Creation Procedure

An account request is made from Human Resources and/or Department managers, in which the employee and the job functions are described. The employee is then contacted by a system administrator to verify the user and the request made to the system administration team.

The employees VPN/SSH and Windows accounts are created as required, see organisational units described below.

Upon creation the password is sent to the individual, the user is required to login immediately and is prompted to change the password on first login.

Account Deletion Procedure

Accounts are deleted when either an employee has left the company or has moved to an organisational unit where access is not required any longer.

The user account is first locked so access is no longer available, and then the systems are investigated for any running processes under the user account that is locked and files owned by the user, where necessary further investigation is carried out and appropriate actions taken.

Procedure

Security Reminders

The IT Security Team shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control.

The IT Security Team may provide such reminders through formal training, e-mail messages, and discussions during staff meetings. The IT Security Team shall be responsible for maintaining appropriate documentation of all periodic security reminders.

The IT Security Team shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

Protection from Malicious Software

As part of the Security Training Program and Security Reminders, the IT Security Team shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:

- Guidance on opening suspicious email attachments, email from unfamiliar senders, and hoax email,
- The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
- Instructions to never download files from unknown or suspicious sources,
- Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
- The importance of backing up critical data on a regular basis and storing the data in a safe place,
- Damage caused by viruses and worms, and
- What to do if a virus or worm is detected.

Password Management

As part of the Security Training Program and Security Reminders, the IT Security Team shall provide training concerning password management.

Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:

- Passwords must be changed every 90 days.
- A user cannot reuse the last 12 passwords.
- Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.
- Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
- A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed.

- Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.
- Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
- Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
- Any employee who is directed by the IT Security Team to change his/her password to conform to the standards shall do so immediately.

Outsourcing

Any outsourced access to the environment will follow the security policy to identify what access is required to allow the necessary outsourced work to be carried out. All accounts will be created in conjunction with the security policy and only for the duration that the outsourced work is carried out by those users.

Upon completion of any outsourced work the user accounts are locked, including remote access to the environment.

All outsourced work will be under a contractual basis and follow the standard NDA and terms of the contract. Any outsourced work will follow a clearly defined set of tasks which will be validated on completion.

Personnel Security

The System/Network Administrators protect the confidentiality, integrity and availability of information, which includes understanding the necessary security requirements for the infrastructure and the remote gaming system.

Responding To Security Incidents & Malfunctions

All security incidents are treated with the highest priority. Each incident is investigated immediately, and an incident report is generated with clear details of the issue, timeline of the investigation and the root cause. All IDS systems proactively alert the security team of any non-compliance regarding policies as well as the monitoring system alerting of any issues with the IDS system malfunctions.

All security devices are based on a High Availability deployment, and 1 malfunction will be covered off by a standby device that is configured to take over automatically and instantly, all security devices are covered by a 4 Hour response time or worse case next business day if a full replacement is required.

Equipment Security

The Internet firewall protects the network from unauthorised access, allowing only the necessary access to internal servers via its policy-based rule set.

Westward Way Tech N. V will have VPN access and access to the internal infrastructure as per our security policy below.

Security Policy

All integration between the software supplier and Westward Way Tech N.V will happen between secure connections created between the two principal firewalls, allowing the possibility of the two systems to be integrated.

The firewall is deployed in a High Availability, full mesh configuration allowing a standby device to take over the primary firewall in circumstances where the primary firewall has failed.

The firewall configuration is automatically synchronised to the standby device (which is identical in specification).

The failover of the firewalls is transparent allowing a failure to be almost unnoticeable.

All collected information that has been stored prior to import is deleted as part of the import process.

Penetration testing is carried out periodically by internal and external means. The penetration test is based on a software program that attempts to penetrate the firewall for external and the internal network vulnerabilities.

System Maintenance Controls (including software)

Any upgrades to the system or patches on the OS go through the required due diligence and testing procedures. Where maintenance is carried out on the OS or network, testing of the patching is carried out prior to releasing this to the production environment.

- All patches are reviewed to understand the detail of any security vulnerabilities and scheduled accordingly.
- Access to the system requires a username and password. Users are assigned to roles which allows them to access only the functionality necessary to that role.
- All files are transmitted over a secure connection when being transferred for maintenance.
- In the case that a third party is required for connection a dedicated connection is used over a secure channel of communication.
- All systems are audited by the IDS system, which sends reports and active alerts if any of the policy rules are not met.
- Financial data is never deleted.

Policy Compliance

The Information Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external

audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

Exceptions

Any exception to the policy must be approved by the Information Security Team in advance. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Version	Date	Details