

META TECH INNOVATIONS B.V.



Information Security Policy

14/08/2024

Table of Contents

Content	Page
Version History	5
Acceptable Use and Ethics	6
Intro	6
Roles and Contractors assigned	6
Policy	6
General Use and Ownership	6 – 7
Security and Proprietary Information	7
Disposal of Equipment	7
Unacceptable Use	7 - 8
System and Network Activities	8 – 9
Email and Communications Activities	9
Enforcement	9
Password Policy	9
Intro	9
Policy	10
Guidelines	10 - 11
Remote Access Policy	12
Intro	12
Policy	12
General	12
Requirements	12 - 13
Acceptable Encryption Policy	13
Intro	13
Policy	13
General	13
Virtual Private Network Policy	13
Intro	13 – 14
Policy	14
General	14
Information Sensitivity Policy	14

Intro	14
Policy	14
General	14 - 15
Network Configuration Guidelines	15
Firewalls	15
Intro	15
Recommendations	15 - 16
Servers	16
Intro	16
Recommendation	16
External Storage Devices	16
Intro	16 – 17
Recommendation	17
Wireless Communications	17
Intro	17
Recommendations	17 - 18
Asset Deployment and Maintenance	18
Intro	18
Recommendations	18
Access Control and Physical Security	19
Intro	19
Recommendations	19
Database Credentials Policy	19
Intro	19
Recommendations	19 - 20
Intrusion Detection Policy	20
Intro	20
Purpose	20
Scope	20
Objectives	20
Recommendations	20
Notification	21
Roles	21

Laptop and Portable Media Security Policy	21
Definitions	21 – 22
Security Policy	22
Laptop Policy	22
Portable Media Policy	22 - 23
Data Classification Policy	23
Data Classification Scheme	23 – 24
Classification Criteria	24 – 25
Asset Owner Responsibilities	25 - 26
Protection from Malware and Viruses: Policy	26
Protection from Malware and Viruses: Technical Controls	26
Protection from Malware: Training and Procedures	26 – 27
Conclusion	27

Version History

Ver.	Description	Author	Date
1.0	Document Created	Danny Vincent Dass	15/08/2024
2.0	Revised Document	Peng Yoon Hun	21/05/2025

Acceptable Use and Ethics

Intro

The purpose of this document is to outline the importance of acceptable use of IT equipment at Meta Tech Innovations B.V. as well as **the integrity, confidentiality and availability of information**. In case of inappropriate use, Meta Tech Innovations B.V. will be exposed to virus attacks, legal issues, services and compromise of network systems.

It is therefore the responsibility of every computer user within Meta Tech Innovations B.V. to know these guidelines, and to conduct their activities accordingly. This document applies also to any 3rd party contractors having remote access to Meta Tech Innovations B.V. systems.

This policy applies to all equipment that is owned by Meta Tech Innovations B.V. or leased to Meta Tech Innovations B.V..

Roles and Contractors assigned

Collaborator	Role	Contact Person	Description
Meta Tech Innovations B.V.	Software Provider / IT Maintenance provider	Meta Tech Innovations B.V. CTO Peng Yoon Hun yoohun@yahoo.com	Responsible for the maintenance of the Software, Network Infrastructure, Servers, Security, Bandwidth and 24/7 Monitoring.
S.S. Netshop Internet Services Ltd.	Colocation Provider	Stefano Sordini – NETSHOP CEO stef@netshop-isp.com.cy +357 2425 0808 +356 2546 6567 +44 203 519 8334	Colocation Provider hosting all production server.

Policy

General Use and Ownership

1. It is the responsibility of the Meta Tech Innovations B.V.'s CSO to safeguard privacy, in this case Meta Tech Innovations B.V.'s CSO who will be responsible of the platform, however users and contractors should be aware that the data they create on the Meta Tech Innovations B.V.'s system remains the property of Meta Tech Innovations B.V.. Because of the need to protect Meta Tech Innovations B.V.'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to Meta Tech Innovations B.V..

2. Any information that users and contractors think or consider it as sensitive or vulnerable must be encrypted to ensure the **confidentiality and integrity of information**.

3. Employees and Contractors 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. In the case of contractors, they should consult the Meta Tech Innovations B.V. CSO.

4. Meta Tech Innovations B.V.'s network and systems are subject to periodic audits to ensure compliance with this policy.

5. For security, network maintenance and **availability of information**, authorized individuals within Meta Tech Innovations B.V. may monitor equipment, systems and network traffic at any time.

Security and Proprietary Information

1. All authorized users and contractors are responsible for the security of their passwords and accounts. Thus, the users and contractors are expected to keep their passwords secure and not share their accounts.

2. **Password-protected screensavers with the automatic activation feature set at 15 minutes or less should be applied through local policies. This is essential for all PCs, laptops and workstations within the internal network at the back office.** Where GPO's and Local Policies are not possible, users should log off by using "control-alt-delete" for Win2k or later editions when the workstation will be unattended.

3. **Laptops should be protected with encryption or any form of data loss protection applications.**

4. **All workstations within the Meta Tech Innovations B.V. network owned by the Meta Tech Innovations B.V. and/or employees and contractors, connected to the internet/intranet/extranet should be protected with an Anti-Virus application as a stand-alone or managed with a console or group policy.**

5. All employees are expected to open all emails with extreme caution. Special attention should be given to emails from unknown sender due to viruses and other malicious software.

Disposal of Equipment

Any equipment, belonging to Meta Tech Innovations B.V., which needs to be disposed of, will be completely destroyed to ensure that there is no data leakage. Before the disposal, the licensee will ensure that appropriate backups are in place to ensure that no data is lost.

Unacceptable Use

The following is a list of activities, which in general, are prohibited. However, employees and contractors with remote access may be exempted from these regulations during the course of their job responsibilities; e.g. in case of a host disrupting the live environment a Meta Tech Innovations B.V. system administrator may have the need to disable its network access.

Under no circumstances is an employee of Meta Tech Innovations B.V. or contractor authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Meta Tech Innovations B.V. owned resources.

The lists below are an attempt to provide a good practice for activities which fall into the category of unacceptable use, meaning that the list below is by no means obligatory.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Under no circumstances the installation/use of “pirated” or other software products that are not appropriately licensed are NOT allowed on the Meta Tech Innovations B.V.’s hosts. “Pirated” software is strictly prohibited. Meta Tech Innovations B.V. is responsible for the authenticity of software installed on the Servers.
2. Unauthorized copying of any copyrighted material for which Meta Tech Innovations B.V. or the end user does not have an active or valid license is strictly prohibited.
3. Passwords should not be revealed to others and accounts are not allowed to be used by others. This includes family and other household members when work is being done remotely from home.
4. 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.
5. Security scanning and port scanning is expressly prohibited within Meta Tech Innovations B.V. network or from any device. Introduction of malicious programs into the network or server is strictly considered as a serious threat (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Using a Meta Tech Innovations B.V. 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.
7. 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, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Packet sniffing is strictly not allowed. In other words 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 or collaborator's normal job/duty.
9. To evade user authentication or security of any host, network or account.
10. Denying or disrupting services to any employee's host within the network.
11. Interfering with or denying service to any user or server within the Meta Tech Innovations B.V. network (for example, denial of service attack), unless this activity is a part of the employee's or collaborator's normal job/duty.

12. 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.

Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

1. 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).
2. 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.
3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
4. Unauthorized use, or forging, of email header information.
5. Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Meta Tech Innovations B.V.'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Meta Tech Innovations B.V. or connected via Meta Tech Innovations B.V.'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any collaborator found to have violated this policy may be subject to end of contract.

Password Policy

Intro

A poorly chosen password may result in the compromise of Meta Tech Innovations B.V.'s entire corporate network, including all its data. As such, all Meta Tech Innovations B.V. employees (including contractors and vendors with access to Meta Tech Innovations B.V. systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords so that **integrity of information is preserved**.

The purpose of the following policies is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Policy

General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a yearly basis.
- All user-level passwords (e.g., email, web, desktop computer, active directory user accounts etc.) must be changed at least every six months. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" or "Domain Admins" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication such IM applications.
- 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).
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

A. General Password Construction Guidelines

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 eight 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 "Meta Tech Innovations B.V." or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

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, !@#\$%^&*()_+|~-=\`{}[]:;';<>?,./)
- Are at least eight alphanumeric characters long and is a passphrase (Oh1seyt0e).
- Is 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: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Employees and contractors should not share Meta Tech Innovations B.V. passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Meta Tech Innovations B.V. information.

Here is a list of "don't's":

- 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, employees and contractors should refer them to this document or have them call someone in the IT Department.

Never use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, Chrome, IE).

Again, do not write passwords down and store them anywhere in the office. Employees and contractors should never store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Computer systems should change passwords at least once every six months (except system-level passwords which must be changed yearly).

If an account or password is suspected to have been compromised, the user or collaborator should report the incident to Meta Tech Innovations B.V. CSO. The CSO may escalate the problem to Meta Tech Innovations B.V..

C. Application Development Standards

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

- 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.

D. Use of SSH for Remote Access Users

Remote access users accessing remotely Meta Tech Innovations B.V. Networks must use a complex password authentication and/or public key authentication via SSH protocol.

Remote Access Policy

Intro

The purpose of this policy is to define for connecting remotely to the Meta Tech Innovations B.V.'s network from any host outside the LAN and therefore **making information available to the right users and avoiding intrusion**. These standards are essential to safeguard the Meta Tech Innovations B.V.'s exposure or loss of confidential data, damage to internal systems and more from unauthorized resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, Fibre connections, VPN, SSH, and cable modems, etc.

Policy

General

1. Employees, contractors and agents with remote access privileges to Meta Tech Innovations B.V.'s corporate network are to ensure that their remote access is given the same attention as the user's on-site connection.
2. The company must ensure that all remote connections are established using secure ports and passwords. A list of requirements is available in the next section.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Meta Tech Innovations B.V.'s network:
 - a. Acceptable Encryption Policy
 - b. Acceptable Use Policy
 - c. Virtual Private Network (VPN) Policy
 - d. Wireless Communications Policy

Requirements

1. It is imperative that secure remote access is strictly controlled. Such control will be enforced via complex password and/or public key based authentication. For a better description for creating strong passwords refer to the Password Policy section.
2. Meta Tech Innovations B.V.'s employees and contractors should not provide their user accounts and passwords not even to family members.
3. Meta Tech Innovations B.V.'s employees or contractors who are granted remote access to the Meta Tech Innovations B.V.'s network must make use of the most up-to-date anti-virus software, this includes personal computers and laptops.
4. Personal equipment (laptops, personal desktops, PDA etc) used to connect to Meta Tech Innovations B.V. network should meet the requirements of Meta Tech Innovations B.V. owned equipment for remote access.

Any employee or contractor found not to have followed the above requirements may be subject to denial of remote access, disciplinary action, up to and including the termination of employment/contract.

Acceptable Encryption Policy

Intro

Employees and contractors who have access to sensitive and confidential data, as defined by the company's CSO, must encrypt the files to protect it from unauthorized disclosure. The purpose of this policy is to provide the users with relevant guidelines concerning data encryption within the Meta Tech Innovations B.V. as well as their responsibilities pertaining to encryption.

Policy

General

1. Encryption programs used must employ proven standards algorithms and must permit properly designated officials within the Meta Tech Innovations B.V., when required, to decrypt the files to acquire the information.
2. Data that is being stored should be encrypted using either a symmetric cryptosystem of the type with a key length of at least 128bits, or, an asymmetric cryptosystem of a type that yields at least equivalent protection strength.
3. Data that is being transmitted must be encrypted using one of the following:
 - a. Web server certificates and web servers which support TLSv1 in strong encryption mode (128 bit or higher symmetric encryption, 1024 bit or higher public key encryption).
 - b. SSL to wrap any clear text protocol/service not encrypted via another method
 - c. Kerberos
 - d. PGP
 - e. Terminal Services
 - f. SSH 2
 - g. PPTP, IPSec

Any contractor found to have violated this policy may be subject to disciplinary action, up to including termination of employment.

Virtual Private Network Policy

Intro

The purpose of this policy is to provide guidelines for Remote Access IPSec or OpenVPN Virtual Private Network (VPN) connections to the Meta Tech Innovations B.V.'s network. This policy applies to all Meta Tech Innovations B.V.'s employees, contractors or any other personnel affiliated with third parties utilizing VPNs to access the Meta Tech Innovations B.V.'s network. This policy applies to implementations of VPN that are directed through an

IPSec Concentrator. The VPN user will also be subject to the conditions and performance constraints of their chosen ISP.

Policy

General

1. It is the responsibility of employees and contractors with VPN privileges to ensure that unauthorized users are not allowed access to Meta Tech Innovations B.V. internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system.
3. VPN gateways will be set up and managed by Meta Tech Innovations B.V. who will be responsible for the Firewall service.
4. All computers connected to Meta Tech Innovations B.V. internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.
5. Users of computers that are not Meta Tech Innovations B.V.-owned equipment must configure the equipment to comply with Meta Tech Innovations B.V.'s VPN and Network policies.
6. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Meta Tech Innovations B.V.'s network, and as such are subject to the same rules and regulations that apply to Meta Tech Innovations B.V.-owned equipment.

Information Sensitivity Policy

Intro

The purpose of this policy is to help the employees determine what information can be disclosed to non-employees and to ensure confidentiality of data. All information within Meta Tech Innovations B.V. should be classified in two main classifications: public and confidential. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes any information on hard copies, any information which is shared orally or visually (e.g. telephony or video conference) and also electronic information. It is imperative that all employees and collaborators familiarize themselves with the information labeling and classification guidelines to follow.

Questions about the proper classification of a specific piece of information should be addressed to the Meta Tech Innovations B.V. CSO.

Policy

General

1. All information which is sensitive to be used to impersonate a person or a process or lead to unauthorized or modification of information fall under the following categories:
 - a. Operational Data
 - b. Personnel Data

- c. Financial Data
- d. Source Code
- e. Technical Information (e.g. Configurations, Connectivity diagrams and patch procedures)

2. **Labeling or Marking information** is at the discretion of the owner of the information. In case the owner or the CSO retains that the specific information has to be labelled the words “**Meta Tech Innovations B.V. Classified**” maybe written on the information in question. Labeling formats are subject to change. Other forms of labels maybe used, for specific business units or departments.

3. All customer related data should be sanitized before using in test and development databases.

4. Only those individuals (Meta Tech Innovations B.V.’s employees or contractors) with approved access and signed nondisclosure agreements can access confidential data. Access will be approved by the CTO.

5. Distribution outside of Meta Tech Innovations B.V. internal mail:

- a. Delivered direct – signature required.
- b. Approved private carriers with acceptable proof-of-delivery services.

6. Any sensitive paper information must be shredded.

7. Any sensitive data on emails should be deleted from mailboxes and stored safely in secure data storage.

8. Any financial information such as credit card numbers stored in databases, logs and backups must be truncated to the last 4 digits.

Network Configuration Guidelines

Firewalls

Intro

The purpose of a firewall is to block all inbound and outbound traffic that has not been expressly permitted by the firewall policy, i.e. traffic that is not needed by the company. This practice, known as “deny by default”, decreases the risk of attack and can also reduce the volume of traffic carried on the organization’s networks.

Recommendations

Firewall policies should only permit appropriate source and destination IP addresses to be used. Specific recommendations for IP addresses include:

- a. Meta Tech Innovations B.V.’s firewall policy should be based on a comprehensive risk analysis.
- b. Policies should take into account the source and destination of the traffic in addition to the content.

- c. Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic proposed by Meta Tech Innovations B.V. and approved by the CSO.
- d. Many types of IPv4 traffic, such as that with invalid or private addresses, should be blocked by default unless explicitly needed.
- e. Meta Tech Innovations B.V. will have policies for handling incoming and outgoing IPv4 and/or IPv6 traffic.
- f. Meta Tech Innovations B.V. will determine which applications may send traffic into or out of its network and make firewall policies to block traffic for other applications.

Servers

Intro

This policy applies to server equipment owned and operated by Meta Tech Innovations B.V., and to servers registered under any Meta Tech Innovations B.V. owned internal network domain.

Recommendations

1. Meta Tech Innovations B.V.'s Servers should be physically located in an access-controlled environment. This co-location service will be provided by co-location centers approved by Meta Tech Innovations B.V..
2. Services and applications that will not be used must be disabled where practical.
3. Virtual Machines with public-facing network connections should be disconnected from the Management Network whenever such connection is not necessary.
4. Security patches must be revised on regular basis and installed on the systems as soon as possible, the only exception being when such patches would interfere with business continuity. At this point these have to be re-scheduled for maintenance windows. Patches will be tested on the Staging Environment before implemented on the live servers.
5. Remote access must be performed over secure channels, e.g. encrypted network connections using VPN connections. See the VPN policy document for more details.
6. Do not use root or Domain Admin accounts for remote sessions. Every employee or collaborator should have his own unique user account with appropriate access level assigned to it.
7. All servers containing confidential (e.g. database servers, application servers and file servers) should be located on an internal network and protected by a firewall.

All above policies apply for any testing environments as well.

External Storage Devices

Intro

This policy is to ensure that the deployment of external storage devices such as USB Memory Sticks and External USB Hard Drives, are maintained and controlled.

It is very well known that removable media are very well-known sources of malware infections and directly tied to the loss of sensitive data. It is therefore the duty of Meta Tech Innovations B.V. to ensure the reduction of acquiring malware infections and minimize the risk to expose sensitive information.

Recommendation

Meta Tech Innovations B.V. staff can only make use of the company's **removable media** in their work computers. **Personal removable devices** cannot be used unless approval from the management is obtained. Sensitive information can be copied to removable devices explicitly when required to perform his or her professional duties.

When sensitive information is copied to a removable device, it must be encrypted in accordance with the company's Acceptable Encryption Policy.

Disposal of Media

Any media that needs to be disposed of will be completely destroyed (if DVD/CDROM are used) or else data sanitization methods such as a data destruction program or file shredder overwrites the data on a hard drive or other storage device to ensure that there is no trace of previous data and hence no data leakage. Before the disposal, the licensee will ensure that appropriate backups are in place to ensure that no data is lost.

Wireless Communications

Intro

This policy is to ensure that the deployment of wireless networking is managed and controlled in a centralized manner to provide functionality whilst maintaining network security with any of Meta Tech Innovations B.V.'s remote offices.

Recommendations

1. Access Points will support the 802.11a, b, g and n standards.
2. Wireless access points that support Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits should be configured to use it.
3. Enable WiFi Protected Access Pre-Shared Key (WPA-PSK), EAP-FAST, PEAP, WEP or EAP-TLS where possible.
4. When enabling WPA-PSK, configure complex secret keys (at least 20 characters) on the wireless client and the wireless access point.
5. Devices with WPA2 support should use WPA2 only. Devices without WPA2 support should use WPA if supported, and WEP only as a last resort.

6. Wireless Access Points configured with WEP keys should be configured with 128-bit strength shared WEP keys, and these should be rotated quarterly at a minimum.
7. Disable broadcast of SSID.
8. Change the default SSID name.
9. Change the default login and password.

Asset Deployment and Maintenance

Intro

For Meta Tech Innovations B.V. to stay current on critical security, stability patches and software changes, regular scheduled systems/network maintenance windows will be scheduled on regular basis. During these maintenance windows, Servers, Routers, Switches, Firewalls and DMZ equipment maybe rebooted and will be generally unavailable for a brief period of time. Thus the purpose of this policy is to list what has to be done in case of such events.

Recommendations

1. All software and hardware configuration records should be documented.
2. System clocks on all equipment should be enabled and all log files should contain date and time stamps.
3. Systems should be regularly revised for unneeded accounts. All employees' accounts that leave the company should be immediately revoked.
4. Inactive accounts should be disabled after a pre-defined period.
5. All changes to firewall configurations must be authorized by the CSO and logged for future reference.
6. All logs related to Firewalls, Routers, and any authentication server logs should be regularly reviewed for unauthorized traffic.
7. Successful and unsuccessful login attempts should be logged.
8. Changes to the live environment should be first tested on the Staging Environment.
9. Any type of changes on the Live Environment which will not involve any downtime should be authorized and logged before being implemented.
10. Any changes on the system, involving downtime on the Live Environment should be scheduled as a maintenance window, and a notification banner should be enabled to notify the customers.

11. Regular vulnerability scans should be performed to identify any devices on the Meta Tech Innovations B.V.'s Network that are open to known vulnerabilities. Such processes can be performed by authorized employees only.

Access Control and Physical Security

Intro

Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent unauthorised access and protection of Meta Tech Innovations B.V. assets – people, information, and infrastructure.

Recommendations

1. Servers and any other Network equipment residing in a datacenter are protected by physical security controls such as the following:
 - a. Automatic Access Control System (AACS).
 - b. Pass or ID system.
 - c. Visitor control.
 - d. Pass activated doors, turnstiles etc.
 - e. Entry and exiting searching.
 - f. CCTV.
2. Meta Tech Innovations B.V. should make use of inventories for media containing sensitive information.
3. All media containing sensitive data, such as backups, should be physically protected from unauthorized access by means of anti-theft safe boxes.

Database Credentials Policy

Intro

This policy 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 Meta Tech Innovations B.V.'s networks.

Recommendations

1. Database user names and passwords may be stored in a file separate from the executing body of the program's code.
2. Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
3. 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.

4. Database credentials may not reside in the documents tree of a web server.
5. Passwords or pass phrases used to access a database must adhere to the Password Policy.
6. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Intrusion Detection Policy

Intro

This policy provides policies to establish intrusion detection and security monitoring to protect resources and data on the organizational network. It provides guidelines about intrusion detection implementation of the organizational networks and hosts along with associated roles and responsibilities.

Purpose

This policy is designed both to protect the confidentiality of any data that may be stored on the mobile computer and to protect the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access.

Scope

This policy covers every host on the organizational network and the entire data network including every path that organizational data may travel that is not on the internet. Paths covered by this policy even include organizational wireless networks. Other policies cover additional security needs of the organizational network and systems.

Objectives

- Increase the level of security by actively searching for signs of unauthorized intrusion.
- Prevent or detect the confidentiality of organizational data on the network.
- Preserve the integrity of organizational data on the network.
- Prevent unauthorized use of organizational systems.
- Keep hosts and network resources available to authorized users.
- Increase security by detecting weaknesses in systems and network design early.

Recommendations

All systems accessible from the internet or by the public must operate IT approved active intrusion detection software during anytime the public may be able to access the system.

All systems in the DMZ must operate IT approved active intrusion detection software.

All host based and network based intrusion detection systems must be checked on a daily basis and their logs reviewed.

All intrusion detection logs must be kept for a minimum of 30 days.

Notification

Any suspected intrusions, suspicious activity, or system unexplained erratic behaviour discovered by administrators, users, or computer security personnel must be reported to the organizational IT computer security office within 1 hour.

Roles

The intrusion detection team shall:

- Monitor intrusion detection systems both host based and network based.
- Check intrusion detection logs daily.
- Determine approved intrusion detection systems and software.
- Report suspicious activity or suspected intrusions to the incident response team.

The incident response team shall:

- Act on reported incidents and take action to minimize damage, remove any hostile or unapproved software, and recommend changes to prevent future incidents. Action shall be based on the approved incident response plan.

Laptop and Portable Media Security Policy

Many employees use portable devices such as personal computers (portable PCs, laptops), Personal Digital Assistants (PDAs), cellphones and smartphones, digital cameras etc., provided by the organization, to work both in and out of the normal work environment. While portable computing devices are undoubtedly convenient, there are increased security risks compared to standard/fixed office IT equipment as a result of:

- Additional vulnerabilities due to their portability and the ways in which they are transported and used (e.g. loss, theft, physical damage; fewer opportunities to apply security patches and antivirus updates);
- Additional threats, especially if used in public places e.g. being directly overlooked, overheard or used by people not authorized to access the information; malware (e.g. virus) infection through portable media or untrustworthy/insecure networks; and
- Additional impacts in some cases (e.g. lost or stolen laptop PCs and access tokens may enable unauthorized remote access the corporate data network; portable storage media typically carry information that is both current and sensitive).

The security of information stored on laptops and portable media is rightly seen as a high-risk area.

This document provides Policy and guidance to cover the security of this area. Care has been taken to ensure that all policies and procedures are compliant with the Lotteries and Gaming Authority of Malta Remote Gaming mandates and in accordance with the ISO 27001:2005 standard.

Definitions

Laptop refers to any of the following:

- Laptop computer, notebook computer, netbook.
- PDA.
- Tablet.

- Phone or smartphone.
- Any other portable computer device running an operating system.

Portable media refers to any of the following:

- CD, DVD, floppy disk, tape, etc.
- External hard disk
- USB memory stick
- Solid-state disk or storage card (e.g. CompactFlash, SD, etc.)
- MP3 or media player.
- Any other device with data storage or data access capability.

Confidential information is any privileged, sensitive or proprietary information that could cause harm or damage to the SPADEGAMING, its staff and management, if compromised through alteration, corruption, loss, misuse or unauthorized disclosure.

Security Policy

All portable information assets must be physically protected against loss, theft, damage and unauthorized access - they must not be left unattended in public areas, unlocked offices, vehicles, hotel rooms, homes etc. without being physically secured e.g. using an approved security cable lock, safe or at the very least tucked away out of sight.

Laptops and portable media, as all corporate IT equipment, must only be used by authorized users for legitimate business purposes.

Laptops and portable media must be logically protected against malware, unauthorized access, unauthorized configuration changes etc. using security products approved for this purpose.

Unauthorized software must not be loaded onto corporate IT equipment, including portable devices and media.

Employees must not interfere with or disable security controls on corporate IT devices, including portable devices and media.

Laptop Policy

This policy applies to laptops, as defined above.

All SPADEGAMING laptops and similar devices must be encrypted at least according to the required specification.

Due to the risk of user error use of unencrypted laptops where confidential information is stored in encrypted folders or files is **not recommended**.

Portable Media Policy

This policy applies to portable media as defined above

Confidential, personal or sensitive information shall not be stored on any non-SPADEGAMING portable medium except as explicitly provided for in contracts with third parties providing goods or services to the SPADEGAMING.

Confidential, personal or sensitive information shall not be stored on any portable medium unless at least one of the following conditions is met:

1. The storage medium is encrypted to at least the SPADEGAMING's required specification.
2. Unencrypted portable media are used only within SPADEGAMING's premises, stored only in a single location and kept securely locked away at all times when not in use.
3. An alternative means of protection providing a stronger level of security is in place, or required by other agencies.

Due to the risk of user error use of unencrypted portable media where confidential information is stored in encrypted folders or files is **not recommended**.

Data Classification Policy

This document defines the data classification policy and scheme used within SPADEGAMING. Data are classed into one of four categories of increasing sensitivity and importance: Public, Internal and Confidential. The classification of data into one of these categories is based on the expected business impact should the Confidentiality, Integrity or Availability (CIA) be compromised. Data cannot have more than one classification.

The data owner is responsible and accountable for determining its correct classification.

The owner is also expected to periodically assess the classification of data under their ownership and adjust the classification where required. Unless otherwise agreed owners should perform an asset classification assessment every two years.

Data Classification Scheme

SPADEGAMING has defined three data classification levels. These are: Public, Internal and Confidential. Data should be given a classification based on their relative importance, value and how restricted their dissemination should be. The relative importance of data or importance of restricting access to it is determined by the data owner.

The three levels of classification are defined as follows:

Level	Description characteristics, and control requirements
0: Public	Level 0 is reserved for all data that are made publicly available by SPADEGAMING. This can include, but is not limited to, published yearend financial statements, information displayed on publicly accessible web sites, marketing material, publicly listed information (such as address or telephone numbers and e-mail addresses) and other types of information that are in no way restricted. Systems or facilities housing public data cannot also contain more restricted assets (i.e. those of higher classification levels) unless the higher classified assets have been ring fenced from the public data with an appropriate set of controls.

	If compromising the CIA of data would result in material financial loss, it cannot be classified as level 0: Public.
1: Internal	Level 1 is the default classification for all SPADEGAMING data that are not made publicly available. All SPADEGAMING staff and affiliated contractors and third parties have access to data classified as 'Internal'. Internal assets are safe-guarded from unauthorised external parties; however it there is no access control requirement for any individual designated as internal to the organisation. This includes all staff members, contractors and third party organisations that have been given access to the SPADEGAMING Internal network or its facilities. If compromising the CIA of data would result in a material financial loss, it must be classified as Internal (level 1) at a minimum. Higher classifications may apply based on the magnitude of loss.
2: Confidential	Level 2 is reserved for the most sensitive and important data within the organisation. Data within this classification are typically protected by the strongest controls and are made available to a select few individuals, almost invariably members of senior management. Level 2 data must be given special consideration as their compromise may threaten continued SPADEGAMING operations. Examples of level 2 data would include merger plans, fraud investigations, strategic plans, R&D material, and proprietary SPADEGAMING IP.

Classification Criteria

All SPADEGAMING data must have a classification based on the expected business impact should either their confidentiality, integrity or availability become compromised. This section defines the criteria that data owners can use as a guide in order to better inform their choice of classification for each of data under their ownership.

- **Confidentiality** is defined as the state where data are available only to those individuals who need to have access them and are approved to do so. Confidentiality is compromised when any unauthorised individual gains access to data.
- **Integrity** is the state where information is whole and generally conforms to its intended purpose and intended state. Any changes or modifications to this information are subject to approval by the appropriate authorities. Integrity is compromised when information is altered, destroyed or otherwise changed by an unauthorised person or unintended event.
- **Availability** is the state where data are made available to the appropriate individuals or process and are done so in accordance to the intended purpose, locations and time frame. Availability is compromised when data are not made available in either in a timely manner, or in its intended locations.

Based on the above definitions of CIA and the requirements of each level of classification in the previous section, the following criteria can be used to guide asset classification:

Level	Criteria
0: Public	An asset should be classified as level 0: public if, - The asset is intended to be freely available to the public. - Compromising the CIA of this asset would not result in a material financial loss to the organisation.
1: Internal	An asset should be classified as level 1: Internal if, - The asset should not be available to the general public. - There is no need to restrict the asset to a specific subset of SPADEGAMING staff. - Compromising the CIA of this asset would lead to a material financial loss to the organisation.
2: Confidential	An asset should be classified as level 2: Confidential if, - Compromising the asset's CIA would threaten the organisation's continued operations. - The asset must be restricted to a particular subset of SPADEGAMING staff. Compromising the CIA of this asset would lead to substantial loss on the part of the organisation, such that it either threatens the continued operation of SPADEGAMING.

If an owner remains uncertain about how data should be classified, the owner should contact SPADEGAMING compliance for further guidance. As a general guideline, all non-publicly available data must, at minimum, be classified as 'Internal' (level 1). Higher classifications are required for more sensitive or valuable data.

Asset Owner Responsibilities

All staff designated as data owners have several responsibilities towards information they have been entrusted with. The responsibilities which are within scope of this policy are:

1. A data owner is responsible for assigning a classification for each asset in their ownership using the requirements and criteria outlined in this policy.
2. When assigning a classification to data, the owner must ensure that they label it in accordance to the SPADEGAMING labelling policy.
3. Each asset owner must make a reasonable effort to ensure that their assets are protected by an appropriate set of controls, proportionate to the assets classification and in agreement with SPADEGAMING risk management practices.
4. Asset owners are free to override materiality thresholds if there is good justification to do so.
5. Asset owners are expected to periodically re-evaluate the classification of assets under their ownership. If deemed necessary the owner can alter the classification of an asset, changing the labelling as required. The owner is responsible for propagating this change across all versions or copies of this asset. Unless otherwise agreed owners should perform an asset classification assessment every two years.

It is assumed that each asset owner is sufficiently knowledgeable and capable of applying the correct classification to an asset. In addition it is assumed that an asset owner is at all times aware of the location of all asset instances under their ownership, be they physical or non-physical.

Protection from Malware and Viruses: Policy

Policy will be established that seeks to prohibit the use of unauthorized software and downloads. The organisation will seek to establish a culture where only approved applications are to be used by employees, and ensure that all web traffic is logged and monitored. This will be made clear in policy, ensuring employees are aware they are accountable for any unauthorized downloads. This acts as both a preventative measure and a detective measure in that malware can quickly be identified and contained.

Policies can take the form of information security policies, acceptable use policies or topic specific policies regarding malware. Whichever form policy takes, it will be clearly communicated to all employees with access to systems on the network and regularly reminded. Employees that are aware of their responsibilities and possible consequences are much more likely to be diligent when using email and web.

Protection from Malware and Viruses: Technical Controls

Technical controls may include anti-virus on both the boundary and on the end user device. This can take the form of basic AV signature based controls through to anti-malware, real-time services. As with all technical controls, configuration and management are key. Signature based detection is reliant on up to date signatures so these will be pushed out to all client/servers on a regular basis. Signatures will also be updated following any new strains of malware being identified, and the organisation will utilize threat feeds from vendors to ensure controls are up to date.

Malware and Viruses can be introduced through email, web or removable media so all channels will be inspected.

Additionally, the organisation will investigate email scanning and web filtering services. Email scanning will inspect SMTP traffic at the gateway for malicious links or attached files, and prevent any suspect email to go through. Furthermore, web traffic will be scanned at the gateway, and URL filtering services will be in place to prevent users browsing to potentially harmful sites.

Finally, removable media controls will be in place to reduce the risk of malware introduced through USB sticks, for example. AV scans will be undertaken on all media connected to devices on the network, and controls will be in place to prevent auto-run. This will ensure that any malware present on devices cannot auto-execute and spread through the network without user intervention.

Protection from Malware: Training and Procedures

Security awareness training is another key control that organisations must consider to protect their network from malicious code. As ever, users are the weakest link when it comes to security and all the technical controls in the world cannot prevent a user clicking a malicious

link in a phishing email. Providing users with regular training on malware, and how to report suspicious emails, files etc. is imperative. This will be tracked, monitored and delivered periodically.

In addition to training, procedures will be established to manage malware incidents when they occur. These will include reporting procedures for users and handling procedures for technical staff. Malware incidents shall be escalated through appropriate channels efficiently, and malware contained, investigated and removed as securely as possible. This may consist of an incident response framework, with individual playbooks for malware based scenarios e.g. ransom ware, virus, Trojans etc. The organisation will invest in red team exercises to test the effectiveness of these responses and ensure that any incidents can be managed effectively.

Conclusion

Standard technical controls are no longer sufficient to manage risk effectively. An effective framework, consisting of technical, procedural, policy and personnel-based controls will be in place and continuously matured. Users must be aware of the risks of malware, and technical controls must be in place to identify any breaches and respond effectively. Policy will state the organisations stance on malware, and procedures will support the principles defined in policy.

The organisation must be able to recover from malware incidents effectively and return to operations as quickly as possible. As this such a critical control, many organisations can spend a long time implementing this control effectively, and this is often recommended as malware can cripple organisations and compromise the confidentiality, integrity and availability of data.