XIMEDES

Information Security and Acceptable Use Policy

Document info	
Release date	21-6-2022
Title	Information Security and Acceptable Use Policy
Version	1.3
Status	Final

XMDS Holding B.V. www.ximedes.com

Lichtfabriekplein 1 2031 TE Haarlem The Netherlands
P.O. Box 2031 2002 CA Haarlem The Netherlands
T: +31 (0)88 248 16 32
K.v.K 534789335

Contents

Document history

Version	Date	Author	Status	Remarks
0.1	20-03-2014	Gijs van den Broek	Concept	
1.0	15-04-2014	Gijs van den Broek	Final	
1.1	12-05-2016	André Flipse	Final	Updated for new Ximedes organization
1.3	21-06-2022	Haritha Khandabattu	Final	Updated changes according to org'22

Document review list

Version	Date	Reviewer	Role
0.1	01-04-2014	J. Portegies Zwart	CISO
1.1	03-05-2016	Gijs van den Broek	Security review
1.3	27-06-2022	Gijs van den Broek, André Flipse	Security review

References

Reference	Title
[1]	Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0

Glossary of Terms

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption. This also involves any other publicly written communication using online services, like social media.
CISO	Chief Information Security Officer. Role assigned to one or more people within the organization responsible for the security of information assets.
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically, the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to Ximedes and/or its customers' reputation or market standing when exposed to unauthorized parties. Examples include, but are not limited to: personal identifiers, financial information, cardholder data and source code.
Security Guideline	A security guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended.
Security Policy	A security policy is typically a document that outlines specific (organizational) requirements or rules that must be met. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities.
Security Standard	A security standard is typically a collection of system-specific or procedural-specific requirements that must be met by everyone; there is no choice.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Ximedes, who do not have a need to know regarding that information.
Removable Media	Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by Ximedes.

1 Introduction

1.1 Purpose

Ximedes[1] develops and maintains security sensitive software solutions for third parties, including solutions that need to be compliant with the Payment Card Industry Data Security Standard (PCI DSS) [1]. The sensitive nature of our work requires us to treat our and our client's data carefully, and design and develop software in such a way that the risk of security-related incidents is minimal.

This document describes the information security and acceptable use policies, guidelines and standards applicable to employees, contractors, consultants, temporaries, and other workers at Ximedes.

Effective information security is a team effort involving the participation and support of every computer user and affiliate who deals with information and/or information systems. It is the responsibility of everyone involved to know these policies, guidelines, standards, and to conduct their activities accordingly.

All staff, managers, and other members of Ximedes and third party service providers who interact with the information owned and/or held by Ximedes are required to read and sign for having received, read and understood the document.

Participants of PCI DSS projects also need to adhere to PCI DSS project specific security requirements. This document is a baseline for all activities within Ximedes , but may be ammended by requirements specific to individual PCI DSS projects, applicable only to the scope of that respective PCI DSS project.

1.2 Scope

The policies in this document apply to the use of information, electronic and computing devices, and network resources to conduct Ximedes business or interact with internal networks and business systems, whether owned or leased by Ximedes, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Ximedes and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Ximedes policies and standards, and local laws and regulation.

1.3 Applicability

Not all statements in this document are mandatory to everyone and/or every activity. The use of various categories of chapters is supposed to clarify to what extent the statements are mandatory.

In particular, please note that:

- **Policy** refers to statements that outline specific (organizational) requirements or rules that must be met. A policy has the highest level of authority in the security document hierarchy;

[1] We use the term 'Ximedes' for all spin-off companies that are under the holding of XMDS Holding B.V.

- **Guidelines** are typically collections of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended;
- **Standards** are typically collections of system-specific or procedural-specific requirements that must be met by everyone; there is no choice.

1.4 Compliance Measurement

The CISO will verify compliance to the security policies through various methods, including but not limited to: business tool reports, internal and external audits and reviews, and provided feedback.

1.5 Exceptions

Any exception to any policy must be approved by the CISO in advance.

1.6 Non-Compliance

Any legal or natural person found to have violated this policy may be subject to disciplinary and/or legal action, in accordance with the regular employee guidelines ('Ximedes Handbook Edition January 2022')

2 Information Security Policy

2.1 Objective

The objective of information security is to ensure the business continuity of Ximedes and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

2.2 Policy

2.2.1.1 The policy's goal is to protect the organization's information assets[2] sufficiently against internal, external, deliberate or accidental threats.

2.2.1.2 The management team of Ximedes has approved this information security policy and is solely responsible for maintaining this document.

2.2.1.3 The security policy ensures that:

a) Information will be protected against any **unauthorized access**;

b) **Confidentiality** of information will be assured;

c) **Integrity** of information will be maintained;

d) **Availability** of information for business processes will be maintained;

e) **Legislative and regulatory** requirements – where applicable - will be met;

f) **Business continuity plans** will be developed, maintained and tested where considered necessary and applicable;

g) **Security awareness training** will be available for all employees;

h) **Secure coding training** will be available for at least all developers and architects;

i) **All actual or suspected information security breaches** will be reported to the CISO and will be thoroughly investigated.

2.2.1.4 Procedures, guidelines and standards exist to support the policy, including virus control and disk encryption measures.

2.2.1.5 The CISO is responsible for providing support and advice during the implementation and maintenance of this document.

2.2.1.6 All (team) managers are directly responsible for implementing the policy and ensuring staff compliance in their respective teams and departments.

2.2.1.7 Organizational and operational risk assessments are executed annually.

2.2.1.8 Compliance with the Information Security Policy is mandatory.

[2] Information can exist in various forms, and includes data stored on computers, transmitted over networks, printed or written on paper, sent by fax, stored on diskettes or magnetic tapes or discussed during telephone conversations.

3 Acceptable Use Policy

3.1 Overview

The purpose of this policy section is to outline the acceptable use of computer equipment at Ximedes. These rules are in place to protect the employee and Ximedes. Inappropriate use exposes Ximedes to risks including malware attacks, compromise of network systems and services, and regulatory, legal and compliance issues.

3.2 Policy

3.2.1 General Use and Ownership

3.2.1.1 Ximedes proprietary information and information owned by customers of Ximedes stored on electronic and computing devices whether owned or leased by Ximedes, the employee or a third party, remains the sole property of Ximedes or the respective customer of Ximedes. You must ensure through legal and/or technical means that proprietary information is reasonably protected against unauthorized access using generally accepted methods of protection.

3.2.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Ximedes proprietary information to the CISO of Ximedes.

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

3.2.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use provided to them, whether owned or leased by Ximedes.

3.2.1.5 For security and network maintenance purposes, authorized individuals within Ximedes may monitor equipment, systems and network traffic at any time.

3.2.1.6 Ximedes reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2.2 Security and Proprietary Information

3.2.2.1 All mobile and computing devices that connect to the internal network through Wi-Fi or VPN must have at least updated anti-malware and updated software patch level.

3.2.2.2 Providing access to any of your Ximedes accounts (and its subsidiaries' accounts) to another individual, either deliberately or through failure to secure its access, is prohibited.

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

3.2.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.2.3 Unacceptable Use

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

3.2.3.2 Under no circumstances is an employee of Ximedes authorized to engage in any activity that is illegal under national, European or other international law while utilizing Ximedes-owned or leased resources.

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

3.2.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

3.2.4.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Ximedes.

3.2.4.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Ximedes or the end user does not have an active license is strictly prohibited.

3.2.4.3 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The CISO of Ximedes should be consulted prior to export of any material that is in question.

3.2.4.4 Introduction of malicious programs into the Ximedes network or any of its servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

3.2.4.5 Revealing your account password to others or allowing use of any of your Ximedes-accounts by others. This includes family and other household members when work is being done at home.

3.2.4.6 Using a Ximedes owned or leased device to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

3.2.4.7 Making fraudulent offers of products, items, or services originating from any Ximedes account.

3.2.4.8 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

3.2.4.9 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

3.2.4.10 Unless for ethical purposes and explicitly pre-approved by the CISO, executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

3.2.4.11 Unless for ethical purposes and explicitly pre-approved by the CISO, circumventing user authentication or security of any host, network or account.

3.2.4.12 Unless for ethical purposes and explicitly pre-approved by the CISO, introducing honeypots, honey nets, or similar technology on a Ximedes network.

3.2.4.13 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

3.2.4.14 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session/device, via any means, locally or via the Internet/Intranet/Extranet.

3.2.4.15 Providing information about, or lists of, Ximedes employees to parties outside Ximedes outside of any job, legal, or business related requirements.

3.2.5 Email and Communications Activities

When using company resources to access and use the Internet, users must realize they represent the company.

3.2.5.1 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).

3.2.5.2 Any form of harassment via email, telephone, social media, or SMS, whether through text, emoticons, frequency, or size of messages.

3.2.5.3 Unauthorized use, or forging, of email header information.

3.2.5.4 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.

3.2.5.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

3.2.5.6 Use of unsolicited email originating from within Ximedes' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Ximedes or connected via Ximedes' network.

4 Password Protection Policy

4.1 Purpose

The purpose of this policy is to establish the creation of strong passwords, the protection of those passwords, and the frequency of change.

4.2 Policy

4.2.1 General

4.2.1.1 All user-level and system-level passwords must conform to the *Password Generation Guidelines* in chapter 4.3.

4.2.1.2 Use of weak passwords – as per section 4.3 – is not allowed for any Ximedes account.

4.2.1.3 Users may never use the same password for Ximedes accounts as for other non-Ximedes access (for example, personal email account, social media, and so on).

4.2.1.4 Where possible, users must not use the same password for various Ximedes access needs.

4.2.1.5 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 to access system-level privileges, and should be based on a public-private keypair for authentication (e.g., SSH authentication keypair), instead of a password.

4.2.1.6 Authentication information for all user-level and system-level accounts should be securely stored using a password manager (e.g., KeePass) which provides encrypted storage and protection of these authentication data.

4.2.1.7 Do not share Ximedes passwords with anyone. All passwords are to be treated as sensitive, confidential Ximedes information.

4.2.1.8 Passwords may never be written down or stored on-line without encryption.

4.2.1.9 Do not reveal a password in email, chat, or other electronic communication.

4.2.1.10 Do not speak about a password in front of others.

4.2.1.11 If someone demands a password, refer them to this document and direct them to the CISO of Ximedes.

4.2.1.12 If an account or password compromise is suspected, report the incident to the CISO of Ximedes and promptly change the password of the account.

4.2.2 Password Change

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

4.3 Password Generation Guidelines

4.3.1 General Password Construction Guidelines

All users should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Are at least eight characters long.
- Contain at least three of the five following character classes:
    - Lower case characters.
    - Upper case characters.
    - Numbers.
    - Punctuation.
    - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.).

Weak passwords have the following characteristics:

- The password contains less than eight characters;
- The password is a meaningful word found in a dictionary.
- 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 "Ximedes", 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).

5 Clean Desk Policy

5.1 Purpose

The main purpose for a Clean Desk Policy is to limit exposure to sensitive information.

5.2 Policy

5.2.1.1 Computer workstations must be locked when the workspace is unoccupied.

5.2.1.2 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

5.2.1.3 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

5.2.1.4 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

5.2.1.5 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

5.2.1.6 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

5.2.1.7 Whiteboards containing Restricted and/or Sensitive information should be erased before leaving the respective (meeting) room.

6 Social Engineering Awareness Guidance

6.1 Purpose

This policy has two purposes: to make employees aware when (a) fraudulent social engineering attacks occur, and (b) that there are procedures that employees can use to detect attacks;

6.2 Policy

6.2.1.1 If one or more circumstances described in section 6.3 is detected by personnel, then the identity of the requester must be verified before continuing the conversation or replying to email, or online;

6.2.1.2 If the identity of the requester cannot be promptly verified, then the person must end the conversation, email, online chat with the requester, and report the episode to the CISO of Ximedes before the end of the business day;

6.3 Guidance

6.3.1.1 Sensitive information will not be shared with an unauthorized individual.

6.3.1.2 Be aware of possible social engineering when either of the following wording is used:

- An “urgent matter”;
- A “forgotten password”;
- A “malware emergency”;
- Any form of intimidation from “higher level management”;
- Any “name dropping” by the individual which gives the appearance that it is coming from legitimate and authorized personnel;
- The requester requires release of information that will reveal technology, source code, passwords, or otherwise sensitive information of Ximedes resources;
- The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, social media, or in person;
- The techniques are used by a person that declares to be "affiliated" with Ximedes such as a subcontractor ;
- The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company;
- The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger);

7 Device Encryption Policy

7.1 Purpose

This policy describes requirements for encrypting sensitive data at rest on Ximedes mobile devices.

7.2 Policy

All mobile devices containing stored sensitive data owned by Ximedes must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, tablets, and cell phones.

7.2.1 Laptops and desktops

7.2.1.1 Laptops and desktops containing stored sensitive data owned by Ximedes must employ full disk encryption with an approved software encryption package. No Ximedes sensitive data may exist on a laptop in clear text.

7.2.1.2 An approved method of encryption to protect data at rest is Bitlocker (using either a password at boot, or a TPM), FileVault, or other equivalent standard-OS supported full disk encryption functionality.

Note: encryption of containers, or otherwise partial encryption of hard drives is not sufficient.
Note: encryption must be applied to all hard drives in a computer.

7.2.2 Tablets and Cell Phones

7.2.2.1 All mobile devices containing stored sensitive data owned by Ximedes must use device-specific storage encryption of all internal media components.

7.2.2.2 Ximedes may employ remote wipe technology to remotely disable and delete any sensitive data stored on a Ximedes-owned or leased tablet or cell phone, which is reported lost or stolen, or is otherwise marked for end of use.

7.2.3 Loss and Theft

7.2.3.1 The loss or theft of any mobile device containing Ximedes sensitive data must be reported immediately to the CISO of Ximedes.

8 Virtual Private Network Policy

8.1 Policy

8.1.1.1 Approved Ximedes employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPN connections to access the Ximedes internal network(s).

Additionally,

8.1.1.2 It is the responsibility of anyone with VPN privileges to ensure that unauthorized users are not allowed access to Ximedes internal networks;

8.1.1.3 Dual (split) tunneling is NOT permitted; only one VPN network connection is allowed;

8.1.1.4 All computers connected to Ximedes internal networks via VPN, or any other technology, must use up-to-date anti-malware software; this includes personal devices;

8.1.1.5 By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Ximedes' network, and as such are subject to the same rules and regulations that apply to Ximedes-owned equipment, i.e., their machines must be configured to comply with this policy document;

9 Removable Media Policy

9.1 Purpose

To minimize the risk of loss or exposure of sensitive information maintained by Ximedes and to reduce the risk of acquiring malware infections on computers operated by Ximedes.

9.2 Policy

9.2.1.1 When sensitive information is stored on removable media, it must be encrypted. This may be achieved using password protected and encrypted archive files (e.g, rar-files);

9.2.1.2 Exceptions to this policy may be requested on a case-by-case basis under discretion of the CISO of Ximedes;