INFORMATION SECURITY POLICY

2018

www.timwe.com

DOCUMENT HISTORY

DATE	STATUS	VERSION	REASON	NAME
24.03.2014	Draft	0.1	First draft	Pedro Evaristo
25.03.2014	Draft	0.2	Refinement	Pedro Evaristo
26.03.2014	Published	1.0	Version for Approval	Pedro Evaristo
12.09.2014	Published	1.1	Minor Correction	ISO27001 Support Team
27.08.2015	Review	1.2	2015 Yearly Refresh	ISO27001 Support Team
09.10.2015	Review	1.3	Annual review process formalized for all related ISMS documentation along with a mitigation of Audit issues.	ISO27001 Support Team
12.10.2015	Update	1.4	Update and approval following the last ISO27001 Management Review Meeting	ISO27001 Support Team
21.07.2016	Review	1.5	2016 Annual Review	ISO27001 Support Team
09.11.2016	Published	1.6	Updated in order to address the 2016 Internal Audit	ISO27001 Support Team
22.01.2018	Published	1.7	Updated in order to address the 2016 Internal Audit	ISO27001 Support Team

GLOSSARY

ACRONYM	DEFINITION
CSO	Chief Security Officer
IS	Information Security
ISMS	Information Security Management System

DOCUMENT CLASSIFICATION	INTERNAL USE ONLY
DOCUMENT CODE	PL02_MS_V1.6_INFORMATION SECURITY POLICY

Table of Contents

1. Purpose and Scope

The current policy aims to protect the information and respective systems from all identified threats, internal or external, deliberate or accidental.

This policy demonstrates the commitment of TIMWE in securing its information and points the requirements to manage and mitigate the risks involved in creation, transport, processing and storage of information from clients and projects, which are the core of TIMWE activity.

The security policy applies to all users with access to TIMWE information, employees or not. Any user with access to technology resources and / or TIMWE information must meet all the applicable rules to its usage, under the terms and conditions stipulated in this and other policies, as well as in any other that may be recorded in additions and / or amendments whatsoever.

The objectives of TIMWE ISMS were defined by top management and overall presented below:

- Integrate Information Security in the business objectives of TIMWE, as distinguishable and competitive factor;
- Solving and reduce information security incidents in a timely manner, that may harm TIMWE business operation and its technological infrastructure;
- Ensure business continuity, always keeping the highest levels of service quality;
- Promote within employees a culture of responsibility and accountability for Information Security;
- Provide regular and transparent performance reporting of the ISMS;
- Keep the ISO27001 certification.

For additional details please consult the ISMS objectives in INTRAWE.

2. Risks and Implications

Any personal computer, workstation or other device that is connected to TIMWE infrastructure is a threat for the infrastructure itself.

Improper use may jeopardize the confidentiality, integrity or availability of information and technological TIMWE infrastructure.

The resolution of security issues increases the operating costs of the technological infrastructure and can cause considerable impacts to TIMWE business operation.

The commitment of each user in following TIMWE Information Security policy can minimize costs and the impacts listed above.

3. Responsibilities

The CSO is responsible for the supervision of ISMS implementation and its policies.

All employees or external entities are responsible for complying with policies that are part of TIMWE's ISMS.

4. Documentation Review

The current policy or any related standards and controls, is subject to a review process and continuous improvement to ensure its continuing suitability and effectively mitigate the risks related with IS and, consequently the business, in compliance with the applicable rules and regulations.

The review of all policies and procedures should be performed at most with 1-year difference or as soon as major changes justify it. The above statement applies for all policies and processes within ISMS.

5. Standards

5.1. Confidentiality and Proprietary Information

All information produced, processed, transmitted and stored within the scope of TIMWE's business is TIMWE exclusive property and may only be copied, reproduced, used, removed or accessed by persons outside the organization, in accordance with the Information Classification procedure.

5.2. Responsibility about Information

The responsibility lies with the IS Steering Committee. The IS Steering Committee is responsible to set access rules according to business needs.

The application of technological security controls and access restrictions is CSO's responsibility, according to the needs expressed by the IS Steering Committee.

5.3. Licensing and Software Installation

All software must be licensed under the name of TIMWE.

In addition to the software installed by default for all users, a list of additional software is installed in each computer according the user's working area. The software list is described in the User Equipment Management document.

The software licensed under the name of TIMWE must be installed on equipment used on professional scope only.

Some licenses may be granted for private use, if it's not for business activity or it is outside the corporate context. Top Management must always grant permission for these particular cases.

Any copy of the Licensed Software can only be made under a Contingency and Recovery plan.

The IS Steering Committee is responsible for the decision of add, change, upgrade or remove any licensed software in the User Equipment Management Technical Document.

5.4. Specialized software

Any employee who requires specialized software should always consult the CSO previously about its usage, and the same must be installed under CTO approval. This policy will ensure software compatibility within operation.

5.5. Prohibited Software

Software that is not necessary for TIMWE business, such as software that may jeopardize the confidentiality, integrity and availability of information and/ or technological systems within TIMWE, should not be installed or executed.

5.6. Data Storage

All information (both business and technical) must be stored on TIMWE systems (OneDrive, INTRAWE, Databases) so that it can benefit from security mechanisms that minimize the risk of downtime, and maximize the confidentiality and integrity of information, such as backups and access control.

Information outside the professional sphere should not be stored on TIMWE systems, and may be deleted without notice.

It is allowed to use mobile storage devices (e.g. pen drives, memory cards) following the rules defined in the Information Classification Procedure.

5.7. Usage rights

The entire TIMWE technological infrastructure composed by networks, software, information and equipment, is owned by TIMWE. Reserves the TIMWE, if it is deemed appropriate, the right to:

- Block and analyze any file or set of unstructured data, stored, processed or in transit, that threats the integrity, confidentiality or availability of TIMWE infrastructure or information;
- Block full or partial access to services (software and/or information), such as E-mail or Internet access, without warning or user's consent, when such usage threats the integrity, confidentiality or availability of TIMWE infrastructure or information;
- Turn off or deactivate any service at any time.

5.8. Passwords

A password allows a system to authenticate a user and assign the necessary permissions for its role.

Please consult the *Password Policy* for additional details.

5.9. E-mail Usage

The usage of Electronic Mail (email) system should be restricted to professional usage within the scope of TIMWE activities.

Its occasional use for private purposes is not prohibited however, yet to be ruled by common sense and moderation, considering abusive, for example, sending mass e-mails, attachments with oversized or inappropriate content.

Suspicious emails, including unsolicited or out of context, should not be opened. Please consult the *Acceptable Use Policy* for additional details.

5.10. Internet Usage

The Internet is an essential tool for TIMWE operation. Internet must be used only for consultation, receipt or publication of information. It should be used sparingly and within the business needs.

The publication of TIMWE information in social networks, blogs, wikis, discussion forums or other types of sites is expressly prohibited, except duly approved by Top Management. Please consult the *Acceptable Use Policy* for additional details.

5.11. Communication Equipment

It can only be linked to TIMWE infrastructure modems, switches, routers, mobile broadband devices, Wi-Fi cards, Wi-Fi devices, or other communication equipment, with the previous CTO approval.

5.12. Antivirus and Security updates

The antivirus installation, configuration, operation, or security updates, may only be performed by IT / Helpdesk department, according the *Security Operations Procedure*.

5.13. Workstation locking (PC's and mobile phones)

Whenever the worker leaves the workstation it must end the session or block access to the workstation, unless it has negative impact on business.

Employees must carry with them service mobile phones all time and have them protected with PIN code.

5.14. Audits

TIMWE will audit and test the equipment on a periodical basis to analyze compliance with security policies and, if necessary, implement corrective measures whenever it's necessary.

5.15. Technical Compliance Reviews

TIMWE will perform technical compliance reviews on an annual basis and its scope should be defined within the ISO27001:2013 Management Review Meeting.

5.16. Approval Method Using Email

Exchange 2010 deployment in TIMWE has the Intra-Org Encryption active, ensuring that mail exchanged between TIMWE e-mails are encrypted. With this level of encryption TIMWE will continue to use the approval method – signing its documents, but acknowledging the email approval as an alternative approved method.

6. Management Commitment

TIMWE Top Management, subscribing the principles recommended in ISO 27001:2013 standards, is committed to:

- Assure and implement the principles outlined in this Policy and its approval, publication and communication to all employees and relevant external parties;
- Assure a strategy to be applied on IS management, aligned TIMWE strategic;
- Secure the creation of an organizational infrastructure and support, ensuring sustainability and the necessary evidences, according with the IS Risk Management;
- Secure the resources for the operation and management of IS processes and activities;
- Promote awareness of workers and external parties about the IS policy, and their share of responsibility on the process;
- Provide regular and transparent performance reporting about IS within TIMWE.

7. Related Documentation

- ISO27001 Scope
- Password Policy
- Information Classification Procedure
- Security Operations Procedure