PO-GL-IT-002

IT Security Policy

7	**09-Dec-25**	**IT Cyber Security & Compliance Director**	**IT Global Director**
		Matt Thompson	**Anders From**
Revision	Revision Date	Document Owner	Document Approver

AMENDMENTS

Rev.	Date	Section	Amendment
7	09-Dec-25	All	Replaced references section with non-compliance and updated policy statements
6	05-Feb-21		Updated new format
5	10-Oct-13		Updated to include content removed from PR-GL-IT-001
4	02-Nov-12		Added Definitions 1.3, References 1.4, Statements 2
3	25-Jun-12		Transferred in to new document template
2	28-Nov-09		Issued in new format
1	19-Nov-09		Issued for use

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

The Company is committed to the security and privacy of company information, regardless of media type, and in accordance with applicable laws and regulations.

This is achieved by adoption of a governed framework of information security controls to provide protection from both internal and external threats, deliberate or accidental.

The purpose and objective of this IT Security Policy is to make Company employees aware of their responsibility to support Information Security controls.

1.2 Scope

This policy applies to any person authorised to access any Company managed computer system or network.

This includes all full-time employees, temporary employees, agency workers, third parties, contractors, and consultants who create, distribute, access, or manage information by means of Company information technology systems, including personal, departmental or corporate computers, networks, and communication services by which they are connected.

It equally applies to individuals and enterprises that, by nature of their relationship to the Company, are entrusted with confidential or sensitive information, such as those offering outsourced services.

1.3 Definition

The definitions for industry or company specific terms and abbreviations used in this document are included within Appendix A of this document.

When used throughout this document, terms below shall have the following meaning:

“Company” shall mean any subsidiary of Subsea7 SA, including joint ventures.

“Employee” shall mean any director, employee or officer of the Company.

“Policy” shall mean the IT Security Policy approved for use

“ISMS” shall mean the Information Security Management System

“Confidentiality” shall mean the term used to prevent the disclosure of information to unauthorized individuals or systems.

“Integrity” shall mean to refer to data that cannot be modified undetectably.

“Availability” shall mean to refer to any information system that to serve its purpose, its information must be available when needed.

“Security control” shall mean to refer to safeguards or countermeasures put in place to avoid, mitigate or minimise security risks.

1.4 Policy Compliance

Compliance Measurement

Compliance to this policy will be verified through various methods, including but not limited to, periodic walk-throughs, monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

Breach of applicable laws or regulation can amount to a criminal offence in many jurisdictions where Subsea7 operates.

Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the Company’s disciplinary policy.

Exceptions

Any exceptions to this policy that are not explicitly defined within must be reviewed and agreed by the Information Security Manager or IT senior management beforehand.

2. POLICY STATEMENT

It is Company policy to ensure that:

- The ISMS and associated security programme will be under continual improvement review

- Computer systems used to store, access and process Company information will be protected by multiple security controls

- Security controls will be implemented to protect the confidentiality, integrity, and availability of Company systems and data in line with their criticality

- Security controls will be implemented and configured to address the current threat landscape

- Details of Company security controls will be documented and subject to regular suitability & maturity assessments

- Information security awareness training program will be available to all users of Company systems to ensure cyber safe behaviours are adopted, reporting procedures are known, and responsibilities are understood

- No attempt should be made to circumvent or subvert any Company IT security control or policy. This could include but is not limited to bypassing, avoiding, or defeating any filtering or monitoring

- IT will monitor, manage, and report on IT incidents including breaches

- All actual and suspected breaches of information security must be reported to the IT Service Desk

- All suppliers to the company must meet a minimum standard of information security, which will be assessed via a Third Party Risk Management process

- Managers are directly responsible for implementing the IT Security Policy within their business areas