Information Security Policy Statement

Confidential/Public/Internal/External

Confidential and proprietary information

This document contains information that is proprietary and/or confidential to the Conectys Group consisting of, ArCoWave SA Luxembourg, Conectys Serv Telecom SRL Romania, Conectys Philippines Inc., Conectys Inc., Conectys Turkey Iletişim Hizmetleri Limited Şirketi, Arcowave Portugal Lda, Conectys Poland Sp. Z O. O. and Arcoman bvba Belgium. It is not to be disclosed, in whole or in part, without the express written authorization of the Conectys Group. It shall not be duplicated or used, in whole or in part, for any purpose other than evaluation.

Document review and approval

Revision history

Version	Author	Date	Revision
1.0	IT Department	8.03.2021	First Draft
1.1	Andrei Stinga	23.08.2022	Updates of the policy

This document has been reviewed by

	Reviewer	Date reviewed
1	Stefan Costel	24.05.2021
2	Andrei Stinga	24.05. 2022
3	Executive Team	24.05. 2022
4		
5		

This document has been approved by

	Name	Signature	Date
1	Arnold Cobbaert – CEO		23.08.2022
2	Brandusa Lupascu – Global VP of Finance & Legal		23.08.2022
3	Oana Bacain - Global VP of Operations		23.08.2022
4	Iulian Bacain – Global VP of Sales & Marketing		23.08.2022
5	Stefan Costel – CTO		23.08.2022

Contents

CONTENTS 3

1. INTRODUCTION 4

1.1 OBJECTIVE 4
1.2 SCOPE 4
1.3 INTENDED AUDIENCE 4
1.4 DOCUMENT MAINTENANCE AND DISTRIBUTION 4

2. POLICY 4

3. APPLICABILITY 5

4. RESPONSIBILITY 5

1. Introduction

1.1 Objective

The objective of information security is to ensure confidentiality, integrity and availability of Conectys, customers and business partners information, to guarantee business continuity and prevent business damage and to minimize the impact of security incidents.

1.2 Scope

This information security requirements document has been prepared to ensure that Conectys is able to support further growth of the business, as well as ensure a consistently high level of customer, supplier, employee, and business-partner service. This document is also intended to support the company reputation for high-integrity and high-quality business services.

1.3 Intended audience

This document applies to the Conectys Group and all its officers, employees, and representatives, including its vendor, suppliers, subcontractors, and others who partner or interact with Conectys, and who rely on the use of Conectys information systems and applications, and/or who have access to, or otherwise, process, personal data, and information on behalf of Conectys.

1.4 Document maintenance and distribution

This document is available for all employees on the Intranet: Documents -> IT -> Global -> Policies and Procedures at this link on SharePoint and will be reviewed at least once every year.

2. Policy

The purpose of the Information Security Policy is to protect the Conectys information assets and the information assets of our customers, as contractually committed, from all threats, whether internal or external, deliberate, or accidental.

It is the Information Security Policy of the organization to ensure that:

- Information will be protected against unauthorized access.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Business requirements for availability of information and systems will be met.
- Regulatory and legislative requirements will be met.

- Business Continuity plans will be produced, maintained, and tested.
- Information security training is mandatory to all staff.
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Head of Security (role covered by position Global IT Planning and Security Manager)
- The Executive Team has approved the Information Security Policy.
- Other security policies and procedures have been developed to support this policy. These include virus and malicious software control, access control, incident control and business continuity.
- Additional standards, procedures and guidelines to the global policies must be produced locally to support the local implementation of the global policies in accordance with local legislation. These local rules define the minimum level of compliance for all employees regarding information security. In such context, the safety and physical security (people and sites) domains contribute to enforce the protection of information.

3. Applicability

All Conectys personnel and suppliers employed under a contract or who have any involvement with information security assets covered by the Scope of the Information Management System are responsible for implementing this policy and shall have support of the Executive Team who has approved the Policy.

4. Responsibility

- The Management of Conectys will implement, maintain, and enforce the Information Security Policy to all staff.
- It is the responsibility of all members of staff to adhere to the Information Security Policy and related standards, procedures, and guidelines.
- The Head of Security has direct responsibility for reviewing the Policy and providing advice and guidance on its implementation.
- All managers are directly responsible for implementing the Information Security Policy within their business areas, and for adherence of their teams.
- Individuals involved in unauthorized activities will be subject to disciplinary action, up to and including termination of employment and to legal proceedings.