ISMS-DOC-05.1 Information Security Policy

Confidentiality	Public (Abbreviated version)
Version	3
Last Reviewed	27 Dec 2021
Next Review	27 Dec 2022
Status	Final version
Document Author	Sharona Van Brussel
Document Owner	Rebecca Dornbusch

Revision History

Version	Date	Revision Author	Summary of Changes
1	07 Feb 2019	Sharona Van Brussel	Creation of document
2	10 Jun 2021	Rebecca Dornbusch	Review of Document
3	27 Dec 2021	Rebecca Dornbusch	Final Version

Contents

1 Introduction

This document defines the information security policy of NewCo Communications.

As a modern, forward-looking business, NewCo Communications recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, NewCo Communications has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally-recognized best practice.

NewCo Communications has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB).

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to NewCo Communications systems.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- *Risk Assessment and Treatment Process*
- *Statement of Applicability*
- *Supplier Information Security Agreement*
- *Information Security Policy for Supplier Relationships*
- *Internet Acceptable Use Policy*
- *Cloud Computing Policy*
- *Mobile Device Policy*
- *Teleworking Policy*
- *Access Control Policy*
- *User Access Management Process*
- *Cryptographic Policy*
- *Physical Security Policy*
- *Anti-Malware Policy*
- *Backup Policy*
- *Logging and Monitoring Policy*
- *Technical Vulnerability Assessment Procedure*
- *Network Security Policy*
- *Electronic Messaging Policy*
- *IP and Copyright Compliance Policy*
- *Records Retention and Protection Policy*
- *Privacy and Personal Data Protection Policy*
- *Clear Desk and Clear Screen Policy*
- *Social Media Policy*