

# P\_ISMS\_DOC\_A5.1\_Policy for Information Security, Privacy and Personal Data Protection



<b>Confidentiality</b>	Internal Documentation
<b>Version</b>	9
<b>Last Reviewed</b>	11 mars 2026
<b>Status</b>	Final version
<b>Document Author</b>	Sharona Van Brussel
<b>Document Owner</b>	Rebecca Dornbusch

## Revision History

<b>Version</b>	<b>Date</b>	<b>Revision Author</b>	<b>Summary of Changes</b>
1	7 févr. 2019	Sharona Van Brussel	Creation of document
2	10 juin 2021	Rebecca Dornbusch	Review of Document
3	27 déc. 2021	Rebecca Dornbusch	Review of Document
4	24 févr. 2023	Rebecca Dornbusch	Review of Document
5	29 nov. 2023	Rebecca Dornbusch	Review of Document
6	17 sept. 2024	Rebecca Dornbusch	Review of Document

7	28 mai 2025	Rebecca Dornbusch	Review of Document
8	15 déc. 2025	Rebecca Dornbusch	Review of Document
9	11 mars 2026	Gloria Rojas Galvez	Review of Document

## Distribution

This document can be viewed on the NCC portal and must be agreed to each year when completing the Security Awareness training.

Name	comment
<a href="#"># Newco Communications – Customer service &amp; business process near- and offshoring</a>	Summary only, full version to be requested at <a href="mailto:informationSecurity@newcogroup.com">informationSecurity@newcogroup.com</a>
NCC Security Portal	full version available to all employees

## Approval

Name	Position	Signature	Date

## Contents

- 1 Introduction
- 2 Policy for Information Security, Privacy and Personal Data Protection
  - 2.1 Scope
    - 2.1.1 Responsibility of all employees
  - 2.2 Framework for Setting Objectives
  - 2.3 Continual Improvement of the ISMS / PIMS
  - 2.4 Information Security Policy Areas
  - 2.5 Application of Policy for Information Security, Privacy and Personal Data Protection

## List of Tables

[Table 1 - Set of policy documents](#)

## 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. As of 2025 NewCo Communications aims not only to expand its ISMS to include a Privacy Information Management System (PIMS) in line with the ISO27701 Standard, but also to expand its certifications to include the Call Center Standard ISO18295.

These standards define the requirements for an ISMS / PIMS based on internationally-recognized best practice. The continued maintenance and improvement of the ISMS / PIMS has many benefits for the business, including:

- Enhanced Data Security and Data Protection
- Risk Management
- Operational Efficiency through streamlined processes
- Compliance with legal and regulatory requirements
- Protection of revenue streams and company profitability
- Ensuring the supply of services to customers
- Protection of Users — ensuring the safety and confidentiality of individuals' data and their rights
- Maintenance and enhancement of shareholder value

NewCo Communications has decided to maintain full certification of the following ISO Standards so that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB):

- ISO 27001 - A standard for managing information security, providing a framework to protect information systematically.
- ISO 27701 - An extension of ISO 27001, focusing on privacy information management to handle personal data processing risks.
- ISO18295 - A standard for customer contact centers, ensuring high-quality customer service and operational efficiency.
- For Sites in Spain only: PCI DSS 4.0.1 - A set of security requirements designed to protect payment card information, with updates clarifying existing requirements and enhancing security measures

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.

## **2 Policy for Information Security, Privacy and Personal Data Protection**

### **2.1 Scope**

This Information Security Management System (ISMS) and Privacy Information Management System (PIMS) scope covers all business processes, information systems, personnel, and

physical locations involved in the delivery of services provided by Newcogroup, with a strong emphasis on the protection of users' data, rights, and safety.

The scope includes the management and protection of information assets—both internal and those entrusted by clients—across the full lifecycle of outsourcing operations, including but not limited to:

- Customer service and support
- IT infrastructure management
- Data processing and storage
- Human resources and payroll services
- Finance and accounting
- Business process management

The ISMS and PIMS apply to all employees, contractors, and third parties who access or process information within the context of these services. The scope encompasses all physical locations, cloud environments, and third-party services used to support these operations.

The ISMS is designed to ensure the confidentiality, integrity, and availability of information in accordance with ISO/IEC 27001:2022, while the PIMS extends this framework to include the protection of Personally Identifiable Information (PII) in compliance with ISO/IEC 27701:2019 and applicable data protection regulations (e.g., GDPR, Moroccan law 0908).

This scope is defined considering the organization's context, interested parties, contractual obligations, and legal and regulatory requirements. Information Security Requirements

It is a fundamental principle of the NewCo Communications Information Security Management System that the controls implemented are driven by business needs and policies that are applicable to all employees shall be made available in a transparent manner to all employees.

NewCo Communications is committed to protecting the confidentiality, integrity, and availability of its information assets. This policy outlines the requirements for maintaining a secure information environment.

### **2.1.1. Responsibility of all employees**

Information security is an important task of all employees within the organization. All employees have the responsibility to:

- All employees must undergo regular information security training to stay informed about the latest security practices and threats.
- Employees are required to be aware and comply with all information security policies and procedures. Non-compliance may result in disciplinary action.
- Employees must report any security incidents, breaches, or vulnerabilities to the Security Team immediately. Prompt reporting helps in quick mitigation and resolution.
- Contribute to risk assessment where required

All employees are empowered to:

- Proactively take measures to prevent or mitigate the occurrence or escalation of information security incidents or data breaches, whenever feasible.
- Promptly report any information security incidents or data breaches that come to their attention.

Please see the document “ISMS-DOC-05.2 Information Security Management System Roles, Responsibilities and Authorities” for specific roles and responsibilities in connection to Security management.

### **Additional Responsibilities for Managers**

In addition to the above, managers and team leaders are required to:

- Ensure that any data subject rights requests (e.g., access, rectification, erasure, restriction, or objection) received within their teams are promptly communicated to the appropriate Security or Privacy function.
- Support the timely handling of such requests by facilitating information gathering and coordination within their teams.
- Promptly inform the Security or Privacy Team of any changes in processing activities within their projects (e.g., changes in scope, purpose, data categories, systems, or third parties) that may impact data protection obligations.
- Ensure that any information security or personal data incident reported within their team is properly documented by completing the designated data breach or incident reporting form without undue delay.
- Verify that all relevant details are accurately captured and escalate the incident to the Security or Privacy Team in accordance with established procedures.

## 2.2 Framework for Setting Objectives

A regular annual cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by NewCo Communications. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- *ISO/IEC 27002 – Code of practice for information security controls*

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

The Statement of Applicability, Risk Analysis and Treatment Plans, along with the SWOT analysis and objectives for the upcoming year, will be defined and updated in Airtable.

## 2.3 Continual Improvement of the ISMS / PIMS

NewCo Communications policy with regard to continual improvement is to:

- **Perform Regular Audits**

Internal and external audits will be conducted annually to assess the effectiveness of the

ISMS / PIMS and identify areas for improvement. Those shall be logged and followed up in  
Airtable

- **Legal and contractual compliance**

Newco Communications is committed to complying with all applicable local, national, and European laws and regulations, including but not limited to data protection legislation such as the General Data Protection Regulation (GDPR EU Regulation 2016/679). In addition, the company ensures adherence to all contractual obligations agreed upon with clients, partners, and third parties.

- **Management Reviews**

Annual management reviews will be held to evaluate the performance of the ISMS and make necessary adjustments.

- **Incident Analysis**

Security incidents will be analyzed to identify root causes and implement corrective actions to prevent recurrence.

- **Measurability**

Make information security processes and controls more measurable in order to provide a sound basis for informed decisions.

- **Proactive Approach**

NewCo Communications is committed to enhancing its security posture by continuously improving the ISMS through the addition of relevant certifications to its portfolio.

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

## 2.4 Information Security Policy Areas

NewCo Communications defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both

within and external to, the organization.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

<b>Policy Title</b>	<b>Areas addressed</b>	<b>Target audience</b>
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.	Users of the Internet service
Cloud Computing Policy	Due diligence, signup, setup, management and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organization or the individual for business use.	Users of company-provided mobile devices
Homeworking Policy	Information security considerations in enabling home working arrangements e.g. physical security, insurance and equipment	Management and employees with approval to work from home after signing the agreement
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system	Employees involved in setting up and managing access control

	and application access control.	
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Employees responsible for protecting the organization's infrastructure from malware
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementing backup regimes
Logging and Monitoring Policy	Settings for event collection. protection and review	Employees responsible for protecting the organization's infrastructure from attacks
Software Policy	Purchasing software, software registration, installation and removal and use of software in the cloud.	Employees responsible for choosing, purchasing and installing software
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment,	Employees responsible for protecting the organization's infrastructure from malware

	hardening and awareness training.	
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Employees responsible for designing, implementing and managing networks
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	All employees
Secure Development Policy	Business requirements specification, system design, development and testing and outsourced software development.	Employees responsible for designing, managing and writing code for bespoke software developments
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software license compliance.	All employees

Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data
Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media.	All employees
Social Media Policy	Guidelines for how social media should be used when representing the organization and when discussing issues relevant to the organization.	All employees

*Table 1 - Set of policy documents*

## **2.5 Application of Policy for Information Security, Privacy and Personal Data Protection**

This policy applies to all employees, contractors, and third-party service providers who have access to NewCo Communications' information assets.

Compliance with this policy is mandatory. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organization's *Employee Disciplinary Process*.

Questions regarding any NewCo Communications policy should be addressed in the first instance to the employee's immediate line manager. Otherwise, any further questions should be directed to [security@newcogroup.com](mailto:security@newcogroup.com) .