POLICY DOCUMENT

Mphasis
The Next Applied

THE INFORMATION SECURITY POLICY

POLICY NO: POL-CRO-000

Policy Owner	Chief Risk Office
Effective date	9-Sep-2025
Supersedes version date	1-Aug-2025

Document Control Information

Document Name	Document Number	Classification	Current Version	Date
The Information Security Policy	POL-CRO-000	Internal	4.7	9-Sep-2025
Prepared By:	Reviewed By:	Approved by	Status	
Kartikey Singh	Amit Mohan Biswal	Pratap Shahane	Approved	

Classification
Classification: INTERNAL • Do not forward or copy data in part or full without explicit permission of Mphasis CRO management • At a minimum, this policy will be reviewed/updated annually

This change history must be updated when any edits are made to this document.

Please contact the CRO team (CRO@mphasis.com) to request changes.

Documented Change History

Version	Date	Approver	Author	Remarks
3.0	9-May-2008	Murali Soundar	Roshan Williams	Changed the document presentation, Included the policy signed by new CEO.
3.1	28-Oct-2010	Murali Soundar	Shakti Nilesh	Change in policy signed by CEO and added ITO accounts under applicability of policy.
3.2	07-Nov-2011	Murali Soundar	Versha Jain	Document reviewed with minor changes.
3.3	05-Nov-2012	Sethu Seetharaman	Pratap Shahane	Document reviewed & updated with minor changes.
3.4	31-October-2013	Sethu Seetharaman	Nigel Pereira	Annual Review and update
3.5	1-Aug-2014	Sethu Seetharaman	Nigel Pereira	Revised as per ISO 27001:2013 requirements,
3.6	28-JUL-2015	Sethu Seetharaman	Pratap Shahane	Annual Review – No changes.
3.7	05-Jan-2016	Sethu Seetharaman	Pratap Shahane	Annual Review – change in policy statements.
3.8	20-Jan-2017	Sethu Seetharaman	Pratap Shahane	Annual Review, No changes.
4.3	2-Aug-2022	Elavarasu AK	Ankur Srivastava	Annual Review, No changes.
4.4	2-Aug-2023	Elavarasu AK	Amit Mohan Biswal	Annual Review, No changes.
4.5	2-Aug-2024	Elavarasu AK	Amit Mohan Biswal	Upgraded to ISO 27001:2022 standard
4.6	1-Aug-2025	Pratap Shahane	Kartikey Singh	Annual Review, No changes.
4.7	9-Sep-2025	Pratap Shahane	Kartikey Singh	Updated the Policy statement to fulfill ESG requirements.

Access List

List of users	Access type	Type of Media	Retention Period
CRO Management	Read/Write/Delete	Soft Copy	Default
CRO Team	Read/Write	Soft Copy	Default
Mphasis employees	Read	Soft Copy	Default

All policies/supplements are subject to local laws where Mphasis and its subsidiaries operate.

These policies/supplements are subject to change without prior notification.

Document Control

Notice of Compliance
Security is the responsibility of everyone affiliated with Mphasis, or directly accessing Mphasis systems, Mphasis data, and data entrusted to the Mphasis by clients or other third parties. The security measures described herein define the basic minimum level of security required for Mphasis systems and information. Non-compliance with the required security measures and behaviors outlined in this policy could pose significant business and legal risk to Mphasis and may create a potential for legal actions that could significantly impact Mphasis's operations and damage its business assets and reputation. Therefore, compliance with this policy and all Mphasis security-related policies, are mandatory conditions for employment for all Mphasis people, as well as any third parties (such as outsourcing providers, contractors, alliance partners, clients, etc.) that access Mphasis systems or data. No one is permitted to bypass the security mechanisms provided by Mphasis systems or infrastructure for any reason. Failure to comply with this policy will be reported and disciplinary action may be taken. Such action may include, but is not limited to, reprimand, financial penalties, termination of employment, and/or legal action. **Note: The Company's policies mandate what must be done and standards tell individuals how to be compliant with policy.**

Exception
All people and all Mphasis systems must comply with the statements in this policy immediately. Where a longer transition is required to achieve compliance, a documented business justification must be submitted with proposed timelines as a Security Exception to CRO for approval. Any exceptions to this Policy must be clearly documented and submitted to the CRO team for evaluation and approval. Only exceptions which have been approved are valid.

Contact Information

For any question regarding this policy, please contact:

Group	Chief Risk Office
Email	CRO@Mphasis.com

INDEX

Contents

1.0 Introduction

This document defines the information security policy of Mphasis Limited.

Compliance with legal and regulatory requirements as a modern, forward-looking business, Mphasis recognizes 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.
To provide such a level of continuous operation, Mphasis 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.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability.
- Ensuring the supply of goods and services to customers.
- Maintenance and enhancement of shareholder value.
- Compliance with legal and regulatory requirements.

Mphasis 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). In addition, the guidance contained in the codes of practice ISO/IEC 27017 and ISO/IEC 27018 has been adopted as these have relevance for Cloud Services.

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

2.0 Scope

This policy applies to all employees, contract staff and Information and Communication Technologies (ICT) of Mphasis Limited and its subsidiaries.

3.0 Information security policy

3.1 Information security requirements

A clear definition of the requirements for information security within Mphasis will be agreed and maintained with the internal business and cloud service customers so that all ISMS activity is focused on the fulfilment of those requirements. Statutory, regulatory, and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of Mphasis Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

3.2 Framework for setting objectives

A regular 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 Mphasis. 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
ISO/IEC 27017 — Code of practice for information security controls-based ISO/IEC 27002 for cloud services
ISO/IEC 27018 — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

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.

3.3 Continual improvement of the ISMS

Mphasis policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) regarding information security
- Make information security processes and controls more measurable to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties, including cloud service customers
- Review ideas for improvement at regular management meetings to priorities and assess timescales and benefits

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

3.4 Application of information security policy

The policy statements made in this document has been reviewed and approved by the top management of Mphasis and must be complied with. 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.

POLICY STATEMENT

Information Security Policy

Mphasis is committed to protect its information assets and provide a secure environment for delivering services to its customers. Mphasis shall strive to secure information by:

- ✓ Establishing and maintaining an effective Information Security Management System.
- ✓ Defining roles and responsibilities pertaining to information security.
- ✓ Performing information security risk assessment periodically.
- ✓ Implementing information security controls to mitigate the identified risks and achieve identified security objectives.
- ✓ Complying with the legal, regulatory and contractual information security requirements.
- ✓ Managing the recovery or continuation of critical business activities and applicable security in the event of a business disruption.
- ✓ Creating a security conscious culture within Mphasis.
- ✓ Continually monitoring and improving the effectiveness of the Information Security Management System.
- ✓ Ensure the confidentiality, integrity, and availability of all information assets through defined controls and continuous validation.
- ✓ Establish processes to continuously monitor the threat landscape, detect anomalies, and respond promptly to information security incidents.

IS POLICY STATEMENT.pdf

Chief Executive Officer (CEO)

Mphasis

The Next Applied

REFERENCE(s)

Control Number	ISO standard reference	Control Objective	Description
5.1	ISO 27001	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Themes and Attributes

Control type	Information security properties	Cyber security concepts	Operational capabilities	Security domains
#Preventive	#confidentiality #integrity #availability	#Identity	#Governance	#Governance_and_Ecosystem #Resilience

Definitions and Acronoyms

Information Security

Information security is all about protecting and preserving information. It's all about protecting and preserving the confidentiality, integrity, authenticity, availability, and reliability of information.

Information Security Management System (ISMS)

An information security management system (ISMS) includes all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organizations use to manage and control their information security risks. An, ISMS is part of a larger management system.

Risk

The concept of risk combines three ideas: it selects an event, and then combines its probability with its potential impact. It asks two questions: what is the probability that a particular event will occur in the future? And what negative impact would this event have if it actually occurred? So, a high-risk event would have both a high probability of occurring and a big negative impact if it occurred. The concept of risk is always future oriented: it worries about the impact events could have in the future.

Risk Assessment

A risk assessment combines two techniques: a risk analysis and a risk evaluation.