




MIT S Global Consulting Pvt. Ltd.

Information Security Policy

Document No.	MIT S-ISMS-PL-01
Issue No. & Date	1.0 & 15/01/2025
Classification of Information	Internal and protected
Revision Status	1.0

	Name	Designation	Signature	Date
Prepared by	Sangeeta M.	General Manager		
Reviewed by	Daxesh Vora	CISO		
Approved by	Sandeep D.	Director		

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date
					<i>1.0 & 15/01/2025</i>

Revision Status

Revision No	Date	Page No.	Clause No.	Brief Description of Revision
1.0	15-01-2025	All	All	The initial issue to comply with the requirements of ISO 27001:2022

All rights reserved.

The information in this document is the property of MITS and is exclusively prepared for MITS.

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of MITS.

Legal action may be taken against any infringement.



	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date <i>1.0 & 15/01/2025</i>

Table of Contents

1. Purpose.....	4
2. Scope	4
3. Roles & Responsibilities	4
4. Abbreviations & Definitions	5
4.1 Abbreviations	5
4.2 Definitions	5
5. Forms	6
6. Information security policy	6
6.1 Information security requirements	6
6.2 Information Security Team	6
6.3 Framework for setting objectives	7
6.4 Continual Improvement of the ISMS	7
6.5 Information Security Policy Areas	8
6.6 Application of Information Security Policy	15
7. Review and Update	15
8. Compliance and Enforcement	15
9. Reference Document	15

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date
					<i>1.0 & 15/01/2025</i>

1. Purpose

This document defines the Information Security Policy of MITS Global Consulting Pvt Ltd.

As a modern, forward-looking business, MITS recognizes at senior levels the need to ensure that its business operates smoothly and without interruption to benefit its clients and other stakeholders.

To provide such a level of continuous operation, MITS 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 practices.

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

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


MITS has decided to maintain full certification to ISO/IEC 27001 so that an independent third party, a Registered Certification Body (RCB) may validate the effective adoption of information security best practices.

2. Scope

This control applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties with access to MITS's systems.

3. Roles & Responsibilities

Roles	Responsibilities
Director	<ul style="list-style-type: none"> • Approve all Mandatory Documents • Approval & Communication Authority.

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date
					<i>1.0 & 15/01/2025</i>

	<ul style="list-style-type: none"> Oversee the implementation of the policy requirements
Employees	<ul style="list-style-type: none"> Adhere to the Policy


4. Abbreviations & Definitions

4.1 Abbreviations

Abbreviations	Expansions
MITS	MITS Global Consulting Pvt Ltd
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
CIA	Confidentiality, Integrity, and Availability

4.2 Definitions

Terms	Definitions
Annex A Controls	Reference controls listed in ISO/IEC 27001 for managing information security risks.
Statement of Applicability	A document specifying which Annex A controls are applied and which are excluded.
Confidentiality	It refers to restricting the access or privilege rights of those who aren't meant to view, access, modify, or transfer the data, hence making it confidential for others to access.
Integrity	It refers to protecting posture or value which makes any set of information valuable. If there is a slight possibility to alter or render any private or confidential data, then its integrity would be compromised.

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date
					<i>1.0 & 15/01/2025</i>

Availability	It refers to the ability to access the data/information when required. The idea of implementing security should be such that the information can be confidential, without losing its integrity and still be available to the dedicated personnel. Any compromise in availability shows that the integrity and confidentiality of the data set are compromised. DDoS attacks are one of the examples of compromised availability.
---------------------	--

5. Forms

Name of the Document	Form No.
NA	---


6. Information security policy

6.1 Information security requirements

- 6.1.1** A clear definition of the requirements for information security within MITS will be agreed upon and maintained with the internal business and cloud service customers so that all ISMS activity is focused on fulfilling those requirements. Statutory, regulatory, and contractual requirements will also be documented and input into 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.
- 6.1.2** A fundamental principle of MITS's Information Security Management System is that the controls implemented are driven by business needs, which will be regularly communicated to all staff through team meetings and briefing documents.

6.2 Information Security Team

Name	Role	Responsibility	E-mail
------	------	----------------	--------

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date <i>1.0 & 15/01/2025</i>

Daxesh Vora	CISO	Overall implementation of Information Security	daxesh@mitsit.net
Daxesh Vora	IT Head	IT Infrastructure Security	daxesh@mitsit.net
Sangeeta M.	ISM	Internal controls, effective use of Policy, Awareness, Internal Audit	sangeeta@mitsit.in


6.3 Framework for setting objectives

- 6.3.1** A regular cycle will be used to set 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.
- 6.3.2** Information security objectives will be documented for an agreed period, 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.
- 6.3.3** Per ISO/IEC 27001, the reference controls detailed in Annex A of the standard will be adopted where appropriate by MITS. These will be reviewed regularly in light of the outcome of risk assessments and in line with the 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.
- 6.3.4** Adopting this code of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

6.4 Continual Improvement of the ISMS

MITS 's policy regarding continual improvement is to:


- 6.4.1** Continually improve the effectiveness of the ISMS

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date
					<i>1.0 & 15/01/2025</i>

- 6.4.2** Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards.
- 6.4.3** Achieve ISO/IEC 27001 certification and maintain it on an ongoing basis.
- 6.4.4** Increase the level of proactivity (and the stakeholder perception of proactivity) about information security.
- 6.4.5** To protect sensitive information, through appropriate authentication practices.
- 6.4.6** Make information security processes and controls more measurable to provide a sound basis for informed decisions.
- 6.4.7** Review relevant metrics on an annual basis to assess whether it is appropriate to change them based on collected historical data.
- 6.4.8** Obtain ideas for improvement via regular meetings and other forms of communication with interested parties, including cloud service customers.
- 6.4.9** Review ideas for improvement at regular management meetings to prioritize and assess timescales and benefits.
- 6.4.10** 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.


6.5 Information Security Policy Areas

- 6.5.1** MITS defines policy in a wide variety of information security-related areas described in detail in a comprehensive set of policy documentation accompanying this overarching information security policy.
- 6.5.2** Each of these policies is defined and agreed upon by one or more people with competence in the relevant area. Once formally approved, it is communicated to an appropriate audience, both within and external to the organization.
- 6.5.3** A comprehensive master list containing the names & document no. of all the policies has been created for reference.


	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date <i>1.0 & 15/01/2025</i>

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


SR.N O	POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
1	Human Resource Security Policy	Recruitment, employment contracts, policy compliance, disciplinary process, termination	All employees
2	Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities, and system and application access control.	Employees involved in setting up and managing access control
3	Acceptable Use of assets Policy	Business use of the Internet, personal use of the Internet, Internet account management, security, and monitoring and prohibited Internet service use cases.	Users of the Internet service
4	Asset Management Policy	Asset Allotment criteria and procedure, Procedure for lost and stolen devices, management of removable media, and disposal of media.	Custodians and owners of assets.
5	Cloud Security Policy	Due diligence, signup, setup, management , and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
6	Risk Management Procedure	A Risk Management Procedure is crucial for an organization specializing in providing	All the department's stakeholders are

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date <i>1.0 & 15/01/2025</i>


SR.N O	POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
		repair and warranty plans for electronics and appliances to mitigate data breaches and ensure security of customer data, safeguarding sensitive information and maintaining regulatory compliance in an increasingly data-driven business landscape.	involved in the management of Customer's PII data.
7	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
8	Logging and Monitoring Policy	Settings for event collection. protection and review	Employees responsible for protecting the organization's infrastructure from attacks
9	Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening, and awareness training.	Employees responsible for protecting the organization's infrastructure from malware
10	Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks, and remote access;	Employees responsible for designing,

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date <i>1.0 & 15/01/2025</i>


SR.N O	POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
		network security management, including roles and responsibilities, logging and monitoring, and changes.	implementing, and managing networks
11	Information Security Event and Incident Management Policy	Effective Information Security Event and Incident Management is essential for an organization specializing in providing repair and warranty plans for electronics and appliances. This is vital to safeguard customer privacy and data integrity, ensuring compliance with regulations and mitigating the risk of data breaches that could compromise customer's sensitive information.	All the employees
12	Electronic Messaging and Information Transfer Policy	Sending and receiving electronic messages, monitoring electronic messaging facilities, and use of email.	Users of electronic messaging facilities
13	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
14	Information security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes, and end of the contract.	Employees involved in setting up and

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date <i>1.0 & 15/01/2025</i>

SR.N O	POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
			managing supplier relationships
15	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
16	Threat Intelligence Policy	A Threat Intelligence Policy is crucial for an organization specializing in providing repair and warranty plans for electronics and appliances. This allows them to proactively identify and mitigate cybersecurity threats, safeguard customer data privacy, and ensure regulatory compliance, thereby preserving the integrity and trustworthiness of systems and customer information.	All the Employees
17	Configuration Management Policy	This document ensures the integrity and traceability of critical software and hardware components, safeguarding customer data from unauthorized access or errors, thereby maintaining compliance with stringent data security regulations.	All the employees

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date <i>1.0 & 15/01/2025</i>


SR.N O	POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
18	ICT Readiness for Business Continuity Policy	The ICT Readiness for Business Continuity Policy focuses on ensuring the availability, resilience, and recovery of IT systems and services during disruptions to maintain business operations.	All the Employees
19	Data Masking Policy	A Data Masking Policy is essential for an organization specializing in providing repair and warranty plans for electronics and appliances to safeguard customer privacy and comply with data protection regulations by obfuscating sensitive customer information while allowing for legitimate data access by authorized personnel. This policy ensures that customer data remains secure and confidential, reducing the risk of data breaches and legal consequences.	All the Employees
20	Change Management Policy	Change Management Process, Categories of Change, Change Advisory Board	Employees involved in development activities and members of the change advisory board.
21	Data Leakage Prevention and	Protection of sensitive data from unauthorized access, accidental leakage,	All employees, IT personnel, and data handlers.

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date
					<i>1.0 & 15/01/2025</i>

SR.N O	POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
	Information Deletion Policy	and ensuring proper data deletion methods.	
22	Clear Desk and Screen Policy	Ensuring sensitive information is not exposed on desks or screens, especially when unattended.	All employees, contractors, and visitors.
23	Protection Against Malware Policy	Safeguarding organizational systems from malware through antivirus solutions, secure practices, and regular updates.	IT personnel and all employees using organizational devices.
24	User Endpoint Device Control Policy	Secure usage, maintenance, and monitoring of endpoint devices to prevent unauthorized access and data breaches.	All employees using laptops, desktops, or other endpoint devices.
25	Remote Working Policy	Establishing secure and efficient practices for employees working remotely, including accessing company systems.	Employees working remotely, IT personnel, and managers.

Table 1: Set of policy documents

In adherence to MITS's commitment to information security, it is to be noted that an Information Security Management System (ISMS) manual has been drafted to serve as a key reference document accompanying this policy. The ISMS manual provides detailed insights into the strategies, controls, and procedures established to safeguard our information assets. For access to the ISMS manual, please refer to the designated location.

	Information Security Policy				
	Doc. No.	<i>MITS-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. & Date
					<i>1.0 & 15/01/2025</i>

6.6 Application of Information Security Policy

- 6.6.1** The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of MITS and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action under the organization's Employee Disciplinary Process.
- 6.6.2** Questions regarding any MITS policy should be addressed to the employee's immediate line manager.

7. Review and Update

This policy will be reviewed and updated annually or as needed to reflect changes in regulations, standards, or organizational processes.

8. Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action as per company's policies and terms of appointment. It is the responsibility of all employees to adhere to this policy and report any potential violations.

9. Reference Document

- ISMS Manual
- Employee Disciplinary Process

Document Note

This document about MITS conforms to the Onsite team of MITS. It is stored in the shared drive in the PDF form. Printed or other electronic copies are for information only.

This document ends here.