GUIDELINE / POLICY	Title	Information Security and Management System (ISMS) Statement of Commitment
	Version	01
	Issue Date	20-09-2024

Document History

Version	Date of Issue	Author	Brief Description of Change	Reviewed By
1	20-09-2024	IT	ISMS Framework	Group CIO

1. Introduction:-

Information Security is a key element of Trident Limited values. It comprises assurance of security of Information Assets belonging to Trident Limited, and the information entrusted to Trident Limited by employees, customers, investors and public at large. Trident Limited is also committed to ensuring compliance to relevant laws and regulations.

2. Objective: -

The objective of the ISMS framework is to ensure that the Business core and supporting operations continue to operate without any disruptions. The Senior Management is committed for the effective Cybersecurity and Information Management System in accordance with its strategic business objectives.

The Information Security Policy at Trident Limited states:

The Senior Management, all Business Units, and all Users processing the Business Information of company shall individually & jointly ensure to protect the Confidentiality, Integrity & Availability of Business Information by adopting & practicing the Information Security Management System as the culture & ethos of the Organisation.

The company shall comply to ISO/IEC 27001:2013 and is committed to protect its Information and Information Systems and has implemented Information Security Management System in accordance with applicable laws and regulations.

3. About ISMS

The ISMS Manual and Information Security Policy details the ISMS and cybersecurity practices of the company. It reinforces that company has an ethical, legal, and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity, and availability. This manual provides the guiding principles and responsibilities necessary to safeguard the security of the organization’s information systems.

4. Coverage

The ISMS manual is applicable to Company “Trident Limited” and all its subsidiaries, its employees, vendors, and contract employees who are the owners, custodians, or users of any Information assets of Company “Trident Limited”

5. Applicability: -

Information Security applies to Information Technology (IT), Data Centre and IT functions of the Company “Trident Limited, Trident Group Sanghera Barnala 148101 India” providing services like Server Management, Network Devices Management, Applications & Database Management, IT Security, Helpdesk Management, Business Continuity planning and Disaster Recovery services.

6. **Cybersecurity and Information Management System Objectives –** Following cybersecurity and Information Management system objectives:

I. Information security policies, standards, guidelines, and procedures are developed to communicate security requirements and guide the selection and implementation of security control measures.

II. Personal accountability and responsibility for information security are incorporated in roles and responsibilities that ensure that every individual applies the applicable information security policies, principles, procedures, and practices in their daily work-related activities.

III. Information security education, training and awareness programs ensure that users are aware of security threats and concerns and are equipped to apply organizational security policies and principles.

IV. Information Assets are classified according to their criticality to the organization enabling an appropriate level of protection.

V. Information Assets are to be used for the intended business purpose only.

VI. Legal, regulatory, and contractual requirements are identified, documented, and followed, such as Information Technology Act 2000 and its subsequent revisions, along with any other applicable laws of land wherever the business is operating.

VII. Ensure adherence to Global Information Security Standard of ISO 27001 and its associated controls.

VIII. Information Security Team of the company is led by the senior & seasoned security professionals.

7. **Reference of existing policies and procedures**

I. **Acceptable Use Policy:** Our Acceptable Use Policy is a set of rules and guidelines that govern the acceptable use of technology and digital resources within the organization. It establishes the rights and responsibilities of users and sets out the permitted uses of technology, while outlining the consequences for improper or unauthorized use.

II. **Access Control Policy:** Our Access Control Policy refers to a set of rules and measures implemented by the organization to regulate and manage access to its systems, networks, and resources. It outlines the guidelines, procedures, and permissions necessary for individuals or entities to gain entry to specific information or perform certain actions within the organization's infrastructure.

III. **Anti-virus & Anti-malware Policy:** Our Anti-virus & Anti-malware Policy is a crucial component of the organization's cybersecurity strategy. The policy outlines the rules and procedures for employees to follow to protect the organization's network, systems, and data from malicious software and cyber threats and includes guidelines for selecting and installing effective antivirus and anti-malware software.

IV. **Backup & Restore Policy:** Our Backup & Restore Policy is a crucial component of the organization's data management strategy and outlines the procedures and guidelines for creating, storing, and recovering data backups in the event of a system failure, data loss, or other unexpected incidents.

V. **Business Continuity Management Policy:** Our Business Continuity Management Policy is a critical aspect of the organization's resilience and sustainability strategy. It involves developing and implementing policies and procedures to ensure the continuity of operations during and after disruptive events, such as natural disasters, cyber-attacks, or pandemics. It outlines organization's commitment to mitigating risks, minimizing the impact of interruptions, and safeguarding the interests of stakeholders.

VI. **Change Management Policy:** Our Change Management Policy document process to review critical changes which are required to be validated and approved by the authorized authority.

VII. **Clear Desk Clear Screen Policy:** Our Clear Desk Clear Screen Policy is a workplace practice that promotes security, organization, and a clutter-free environment. The policy requires employees to ensure that their desks are free from any sensitive information or documents at the end of each working day. Additionally, it encourages employees to lock their computers or screens when they are away from their desks, minimizing the risk of unauthorized access or data breaches.

VIII. **Compliance Policy:** Our Compliance Policy set guidelines and procedures to ensure compliance with legal and regulatory frameworks.

IX. **Cryptographic Controls Policy:** Our Cryptographic Controls Policy set guidelines and procedures to implements secure and effective use of cryptographic controls which are measures used to protect information by applying encryption and decryption techniques.

X. **Email Security Policy:** Our Email Security Policy governs guidelines to protect sensitive and confidential information from unauthorized access, data breaches, and cyber-attacks. It outlines guidelines and procedures that employees must adhere to when using corporate email systems, ensuring the confidentiality, integrity, and availability of email communication.

XI. **HR Security Policy:** Our HR Security Policy sets guidelines and procedures to protect the security of the organization’s human resources data and ensure the privacy of its employees. This policy encompasses areas such as data protection, access control, incident response, and employee awareness training.

XII. **Incident Management IT Helpdesk Policy:** Our Incident Management IT Helpdesk Policy is a critical component of the organization's IT infrastructure. The policy outlines the procedures and guidelines for managing and resolving incidents through well managed ticketing application. It ensures that there is a standardized and efficient approach to handling and resolving technical issues, minimizing the impact on the organization's operations.

XIII. **Information Asset Classification & Handling Policy:** Our Information Asset Classification & Handling Policy helps identify and categorize the organization's information assets based on their value, sensitivity, and criticality. It outlines the procedures and guidelines for handling, storing, and sharing information to prevent unauthorized access, loss, or misuse.

XIV. **Information Security Policy:** Our Information Security Policy outlines the organization's approach to protect its information assets from unauthorized access, usage, disclosure, disruption, modification, or destruction.

XV. **Information Transfer Policy:** Our Information Transfer Policy outlines the guidelines and procedures for sharing and disseminating important information within or outside the organization. This policy sets out the responsibilities and roles of individuals involved in this process.

XVI. **ISMS Definitions & References:** The document defines various terminologies used in information security management system policies and procedures.

XVII. **IT Asset Management Policy:** Our IT Asset Management Policy is crucial for efficiently managing the IT Assets This policy outlines the procedures and guidelines for acquiring, allocating, monitoring, and disposing of various IT assets within the organization.

XVIII. **Network Security Policy:** Our Network Security Policy set guidelines and procedures to protect our digital infrastructure from unauthorized access, data breaches, and other potential threats.

XIX. **Password Policy:** Our Password Policy set guidelines and requirements to ensure security of its digital resources and aims to protect sensitive information from unauthorized access and minimize the risk of data breaches

XX. **Physical & Environment Security Policy:** Our Physical & Environmental Security Policy is essential for the organizations to protect its facilities, assets, and personnel from various threats. The policy aims to create a secure environment by implementing measures such as access controls, surveillance systems, and disaster preparedness plans.

XXI. **Removable Media Policy:** Our Removable Media Policy set guidelines on all removable media storage devices to prevent breach of confidential information.

XXII. **Supplier Security Policy:** Our Supplier Security Policy aims to protect the organization's asset that are accessible by suppliers or third-party vendors.

XXIII. **System Acquisition, Development & Maintenance Policy:** Our System Acquisition, Development & Maintenance Policy outlines the procedures and guidelines for acquiring, developing, and maintaining systems and applications within the organization.

XXIV. **Technical Vulnerability Management Policy:** Our Technical Vulnerability Management Policy outlines the procedures and guidelines for identifying, assessing, mitigating, and reporting vulnerabilities within the organization's systems and networks. The policy provides a standardized approach to ensure that vulnerabilities are addressed promptly and effectively. We also involve external agencies/ expertise for unbiased & detailed vulnerabilities assessment.

XXV. **Work from Anywhere Security Policy:** Our Work from Anywhere Security Policy sets guidelines and protocols designed to ensure the security of remote work environments. It is crucial to address potential security risks that may arise from employees working from remote locations.

Responsibility Matrix: -

1.	Review	Group CIO
2.	Implementation/Execution	IT Head
3.	Monitoring	Group CIO
4.	Auditing	Audit Committee
5.	Ownership	Group CIO

For Trident Limited

DEEPAK NANDA

Digitally signed by DEEPAK NANDA
Date: 2024.09.20 20:03:44 +05'30'

Deepak Nanda
[Managing Director]

Disclaimer: - This Document is to the confidential property of the Trident Limited and shall not be reproduced, copied, disclosed to others, or used otherwise without the prior written permission of Trident Limited.