INFORMATION SECURITY & DATA PROTECTION POLICY

APPROVED BY CEO
DAS CERTIFICATION PRIVATE LIMITED
EFFECTIVE DATE: 24 OCTOBER 2025
VERSION: 1.0
NEXT REVIEW DATE: 23 OCTOBER 2025

www.dascert.com

EFFECTIVE DATE: 24 OCTOBER 2025
VERSION: 1.0
NEXT REVIEW DATE: 23 OCTOBER 2025

Purpose

This policy establishes the principles and framework for safeguarding all forms of information assets, including personal data, collected, stored, processed, or transmitted by DAS Certification (Pvt.) Ltd. It aims to ensure confidentiality, integrity, availability, and compliance with applicable laws and standards.

Scope

This policy applies to all employees, contractors, consultants, trainees, and any third-party service providers who access or process DAS information systems, networks, or data.

Policy Statement

DAS Certification (Pvt.) Ltd. is committed to:

- Protecting the security and privacy of its data and that of its clients, employees, and partners.
- Complying with all relevant legal, regulatory, and contractual requirements, including ISO/IEC 27001 and applicable data protection laws.
- Preventing unauthorized access, disclosure, alteration, or destruction of information.

Roles and Responsibilities

- Top Management: Provide leadership, allocate resources, and ensure enforcement of this policy.
- Manager Compliance- Oversee implementation of security controls, monitoring, and risk management.
- All Employees: Comply with security policies and procedures, report incidents, and protect data entrusted to them.

Information Security Objectives

- Ensure only authorized individuals have access to relevant information.
- Maintain the accuracy and completeness of data and prevent unauthorized modification.
- Ensure availability of information to authorized users when needed.
- Establish controls for physical, network, and logical access.
- Prevent data breaches, cyberattacks, or loss of sensitive information.

Data Protection Principles

DAS shall ensure personal and confidential data is:

- Lawfully and fairly processed with clear purpose.
- Accurate and up to date, retained only as long as necessary.
- Protected from unauthorized access, misuse, loss, or destruction.
- Subject to user rights, including the right to access, correct, or delete their data.

Access Control

- Users are granted access based on job roles (principle of least privilege).
- All user activities are logged and monitored where necessary.
- Strong authentication (e.g., passwords, biometrics, 2FA) is required for access to sensitive systems.

Physical and Network Security

- Secure areas are protected by access controls and surveillance.
- Company laptops and mobile devices are encrypted and password-protected.
- Firewalls, antivirus, intrusion detection systems (IDS), and regular patching are implemented.

Data Backup and Recovery

- Regular backups are conducted and stored securely offsite.
- Disaster recovery and business continuity plans are in place and periodically tested.

Training and Awareness

- All employees receive induction and periodic training on information security and data protection.
- Refresher training is provided annually or after major incidents/changes.

Incident Reporting and Response

- All security breaches or suspected data leaks must be reported immediately to the Information Security Officer.
- Incidents are investigated, documented, and corrective actions are implemented.

Third-Party & Vendor Management

- Third parties handling DAS data must sign confidentiality agreements and comply with this policy.
- Vendor security practices are evaluated before engagement.

Compliance and Review

Non-compliance with this policy may lead to disciplinary action, including termination or legal consequences.

This policy shall be reviewed annually or as required by changes in legal, regulatory, or business environments.

Approved by:
CEO
DAS Certification (Private) Limited