"Information Management s Classification Policy"

Company: DAS TECHNOLOGY SERVICES LLC
Author: Shaheer Nawaz, IT Support Specialist
Review Cycle: Annual
Version: V1.1
Approved By: IT Security Department

---

1. Purpose

The purpose of this policy is to ensure that all information assets of DAS TECHNOLOGY SERVICES LLC are properly protected through appropriate classification, handling, and storage based on their sensitivity, value, and criticality to the organization.

---

2. Scope

This policy applies to all employees, contractors, and third-party partners of DAS TECHNOLOGY SERVICES LLC who handle, process, or manage company data.

---

3. Information Classification Levels

All information assets must be classified into one of the following categories:

- **Confidential**
  - **Description**: Highest level of sensitivity.
  - Examples: User credentials, financial records, personally identifiable information (PII), intellectual property, legal documents.
  - **Handling**: Must be encrypted in transit and at rest; access restricted to authorized personnel only.
- **Internal Use Only**
  - Description: Business-sensitive data not intended for public disclosure.

- Examples: Internal project plans, non-public financials, internal emails.
- Handling: Share only within the company; protect with role-based access controls.

❖ **Public**

- Description: Approved for public release.
- Examples: Marketing materials, public website content, job postings.
- Handling: Can be freely shared externally with no restrictions.

---

4. Roles and Responsibilities

➢ **Information Owners**

- Classify data appropriately.
- Approve access to their information assets.
- Ensure data retention and disposal requirements are followed.

➢ **IT Department**

- Implement technical controls to enforce classifications.
- Provide encryption, access control, and monitoring solutions.
- Train staff on secure data handling practices.

➢ **All Employees**

- Follow this policy and related procedures.
- Protect data in accordance with its classification.
- Report any unauthorized access or data mishandling.

---

5. Data Handling Requirements

Classification	Storage	Access	Transmission	Disposal
Confidential	Encrypted, secured servers	Restricted to specific roles	Encrypted (TLS/SSL)	Shredding, secure wipe
Internal Use	Authorized internal systems	Employees only	Internal VPN/email	Normal deletion or shredding
Public	Public servers, cloud	Open access	Open transmission	Normal deletion

---

6. Data Retention

All data must be retained in accordance with legal, regulatory, and operational requirements. Data not needed should be securely deleted as per its classification.

---

7. Data Segmentation in Multi-Tenant Environments

DAS TECHNOLOGY SERVICES LLC enforces strict controls to protect client information, including T-Mobile Protected Information, within multi-tenant environments. These controls include:

- **Logical Segmentation**: Customer data is logically separated using role-based access controls (RBAC) and unique security identifiers.
- **Encryption**: All customer data is encrypted in transit (TLS 1.2 or higher) and at rest using AES-256 encryption standards.
- **Access Control**: Only authorized personnel with a documented business need are granted access to T-Mobile Protected Information.
- **Continuous Monitoring**: Systems handling multi-tenant data are monitored 24/7 for unauthorized access attempts.
- **Compensating Controls**: Where physical segregation is not feasible, DAS TECHNOLOGY SERVICES LLC implements encryption, multi-factor authentication, and network segmentation to safeguard data.

These measures ensure that T-Mobile Protected Information is isolated from other client data and appropriately protected even in shared environments.

8. Policy Violations

Non-compliance with this policy may result in disciplinary action, up to and including termination, and potential legal consequences.

G. Review and Maintenance

This policy shall be reviewed annually or after any major security incident. Updates must be approved by the IT Security Department.

10. Acknowledgment

All employees must read, understand, and acknowledge this policy upon hire and annually thereafter.