“Physical &s Remote Security Policy”

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

---

1. Purpose

The purpose of this policy is to establish physical security requirements and practices to protect DAS TECHNOLOGY SERVICES LLC personnel, infrastructure, and information assets from unauthorized physical access, damage, or interference.

---

2. Scope

This policy applies to all physical locations operated or owned by DAS TECHNOLOGY SERVICES LLC, including offices, data centers, and remote workspaces that store or access company data.

---

3. Physical Security Objectives

- Prevent unauthorized physical access to company resources.
- Ensure environmental protection for IT infrastructure.
- Detect and respond to physical security incidents.
- Promote a culture of safety and vigilance.

---

4. Key Physical Security Controls

4.1 Facility Access Control

- All facilities must use access control systems (keycards, biometric scanners, etc.).
- Access is restricted based on job roles and responsibilities.

- Visitors must be pre-approved, logged, and escorted at all times.

4.2 Surveillance s Monitoring

- CCTV cameras are installed at all critical entry/exit points and data-sensitive areas.
- Footage is retained for a minimum of 90 days.
- Security logs are reviewed regularly.

4.3 Server Room/Data Center Security

- Entry to server rooms is limited to authorized IT personnel.
- Racks must be locked, and sensitive hardware must be protected with tamper-evident seals.
- Environmental sensors (temperature, humidity, smoke) must be deployed and monitored.

4.4 Workplace Security

- All employees are issued company ID badges and must wear them during working hours.
- Workstations must be locked when unattended.
- Confidential materials must be secured in locked drawers or cabinets.

4.5 Remote Work Protections

- Employees must work in a private and secure location when accessing company data remotely.
- Company devices must not be left unattended in public or shared spaces.

---

5. Equipment and Asset Security

- All company-owned equipment must be tagged and inventoried.
- Portable devices must be locked away when not in use.
- Lost or stolen devices must be reported immediately to IT and HR.

---

6. Environmental Safeguards

- Fire suppression systems must be installed in data rooms.
- Uninterruptible Power Supplies (UPS) must be used to protect critical systems.
- Emergency evacuation plans must be displayed and reviewed regularly.

---

7. Training and Awareness

- All employees receive physical security training during onboarding and annually.
- Drills (fire, emergency evacuation) are conducted periodically.

---

8. Violations and Enforcement

- Any breach of physical security protocols will be investigated.
- Disciplinary actions may include suspension, termination, or legal action.

G. Policy Review and Updates

This policy will be reviewed annually or after significant changes to facility operations or a reported security incident.