Defense in Depth Security Control Types

"Defense in Depth" is a multi-layered security strategy integrating **administrative, technical, and physical controls** to ensure **if one fails, others protect.** By implementing multiple controls, organizations can protect against a variety of threats, from cyber-attacks to internal breaches, ensuring that critical systems and data remain secure.

Administrative Controls

Admin controls manage user behavior and operations through policies, training, and audits.

Policies & Procedures
Standards for organizational activities, including security guidelines.

Personnel Security
Hiring and managing staff with security-focused processes.

User Training & Awareness
Educating staff on security best practices and potential threats.

Audit and Monitoring
Regularly reviewing security practices for policy compliance.

Access Control Policies
Defining roles for resource access based on organizational roles.

Incident Response Plans
Handling security incidents from identification to recovery.

Physical Controls

Physical controls protect assets via locks, barriers, surveillance, and access management.

Environmental Controls
Systems to protect against fire, flood, and other hazards.

Surveillance Systems & Security Guards
Cameras and monitoring for security and safety.

Secure Facility Access
Restricted access to buildings using keycards or biometrics.

Physical Barriers
Fences, gates, and locks to prevent unauthorized entry.

Visitor Management
Processes to control and monitor visitor access.

Secure Equipment Areas
Protected zones for sensitive or critical equipment.

Technical Controls

Technical controls safeguard IT via firewalls, encryption, antivirus, and access systems.

Firewalls
Systems to block unauthorized network access.

Intrusion Detection Systems
Monitoring networks for suspicious activities.

Encryption
Protecting data in transit and at rest.

Antivirus Software & Patch Management
Protection against malware and viruses plus security updates.

Data Backup
Regular backups of critical data for recovery purposes.

Access Control Systems
Restricting user access to systems and data.

LEARNING TREE INTERNATIONAL

www.learningtree.com/topics/cybersecurity