Securing IT Assets

Access Control -> Granting or deny specific requests to obtain and use information an related information processing services. Users are identified and granted certain rights to access and perform functions with information systems, networks or databases

Least Privilege -> Only have access to you need, if you just use the read administration to work you do not need edit administration (necessary to perform their duties)

Application Allow List -> Only approved applications could be installed

Decommissioning -> It involves safely and systematically retiring theses assets to ensure that no security vulnerabilities are introduced during or after the process

Hardening -> Measures and practices taken to reinforce the security of a system or network, the goal it to reduce vulnerabilities and minimize the attack surface

- Encryption
- Disabling Ports/Protocols -> Disable unused or unsecure ports/protocols (Think like Least Privileges but for ports/protocols)
- Endpoint Protection -> Antimalware and EDR
- HIPS (Host Intrusion Prevention System) -> It monitors and analyzes systems behavior and configuration
- Change Default Passwords
- Removal of Unnecessary Software -> Think like Least Privileges but for software installed in the device

Uninterruptible power supply (UPS) -> Backup power in case of sudden power loss, allowing critical systems to remain operational for a short period
Generators -> Ensuring operational continuity during extended power outages by providing a reliable source of backup power
Power converters -> Convert electrical power from one form to another (AC to DC or vice versa)
Power regulators -> Stabilize voltage levels to protect sensitive equipment from power surges or fluctuations