Physical Security Protections

Purpose:

Protect state systems and assets by controlling physical access and implementing controls to protect the environment in which they are housed.

Why it's important:

Physical security protections limit access to buildings, servers and equipment and minimizes potential security breaches. Monitoring all physical security controls enables rapid detection and response to physical security incidents.

Target audience:

All personnel

Overview:

- Develop and maintain a list of personnel with authorized access to controlled areas where the state information system resides. This list shall be reviewed and updated quarterly.

- Enforce physical access where the state information system resides.

- Maintain visitor access records to controlled areas where the information system resides. Review visitor access records monthly and maintain visitor logs.

- Implement physical access controls such as locked wiring closets, safeguards for workstations, and limit access to state information system output devices. Restrict access to network jacks and devices. Protect power equipment and cabling from damage or destruction.

- Provide emergency power and emergency shut off of power to the state information system and components.

- Employ fire detection and suppression systems that are supported by an independent energy source.

- Maintain temperature and humidity levels in data centers, server rooms and computer rooms.

- Protect state information systems from damage resulting from water leakage with master shutoff or isolation valves that are easily accessible.

Control access where the state information system resides with keys, locks, combinations, card readers, and/or guards.
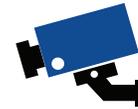
Provide cameras, monitored by guards, to control access to areas within designated as publically accessible.

Develop procedures to easily distinguish between onsite personnel and visitors.

Monitor physical intrusion alarms and surveillance equipment.

Employ and maintain automatic emergency lighting in the event of a power outage.

Employ fire detection systems that activate automatically and notify emergency responders.

For more information about this IT Security Policy, contact SecurityPolicies@azdoa.gov.

ADOA-ASET
Arizona Strategic Enterprise Technology

07.07.14