

SAM – INFORMATION SECURITY
(Office of Information Security)

PHYSICAL SECURITY
(Revised 6/14)

5365

Policy: Each state entity shall establish and implement physical security and environmental protection controls to safeguard information assets against unauthorized access, use, disclosure, disruption, modification, or destruction. Physical security and environmental controls shall include management and maintenance of:

1. Facility entry controls and badging systems for personnel and visitors;
2. Equipment and media handling/destruction processes;
3. Building emergency procedures;
4. Screening and/or background check processes;
5. Ventilation and temperature control systems; and
6. Fire suppression, water damage prevention, and electrical power fluctuation or failure detection systems.

Each state entity shall issue physical access authorization credentials to state entity personnel and visitors, as appropriate. Personnel with long-term physical access authorization credentials are not considered visitors. Authorization credentials include, but are not limited to, badges, identification cards and smart cards. The strength of authorization credentials necessary, including level of forge-proof badges, smart cards, or identification cards, shall be determined through a risk assessment.

Each state entity shall monitor physical access to information systems to detect and respond to physical security incidents; review physical access logs and, upon occurrence of an incident, coordinate results of reviews and investigations with the state entity incident response capability.

Implementation Controls: NIST SP 800-53: [Physical and Environmental Protection \(PE\)](#)