		Effective:	7/1/2017
		Last Review:	7/1/2017
Title:	Equipment Security	Next Review:	Annually
Number:	ISP-142		
Version:	1.0	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure that State of Alaska (SOA) information processing systems and SOA information assets are appropriately protected from physical and environmental threats.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Equipment must be secure and protected; and
- Access controls must be implemented.

5.1. Equipment Must be Secure and Protected

5.1.1 Secure Areas

Personnel tasked with information system deployment responsibilities must ensure that SOA information systems are deployed within a secure facility such as a data center, storage cabinet, collocation facility, or other approved area. Business Managers must evaluate the risks associated with physical, environmental, geopolitical, or other threats and deploy additional security controls as needed to mitigate these threats in a manner commensurate to the classification of the information.

5.1.2 Cables and Wiring

Personnel tasked with information system deployment responsibilities must:

- Ensure that data communication links such as telephone cables and network cables are appropriately protected to prevent unauthorized access to sensitive information.
- Ensure that power cabling or other cabling required to support information systems is protected from unauthorized tampering or disturbance.
- Not deploy cabling where confidential or SOA internal only information must travel (e.g., in public areas, lobbies or commonly shared rooms) in areas outside of SOA control.

5.1.3 Wiring Closets

Personnel must ensure that wiring closets, telephone junction boxes, or other supporting infrastructures are protected from unauthorized access through the use of physical security controls.

5.2. Access Controls Must be Implemented

5.2.1 Physical Access Controls

Personnel tasked with information security oversight responsibilities must implement controls to ensure that physical access to secure information processing facilities, data centers and wiring closets is protected from unauthorized physical access.

5.2.2 Logical Access Controls

Personnel tasked with information security oversight responsibilities must implement administrative and technical controls to ensure that only authorized personnel are provided logical (e.g., administrative console) access to information systems containing sensitive information.

5.2.3 Auditing of Controls

Personnel tasked with information security oversight responsibilities must implement proper auditing controls to identify personnel accessing secured or controlled areas. This would include either automated access control logging or physical “paper” logs which personnel must sign when entering and leaving a controlled area.