

SUBJECT: INFORMATION SECURITY

NOTE:

There is a Collective Bargaining Agreement (CBA) between the State of Washington and the Washington Federation of State Employees (WFSE) that applies to represented employees.

When a topic is covered in the CBA, the policy on that topic applies only to non-represented employees. If the agency's policy conflicts with the CBA, the CBA supersedes the policy for represented employees. Where there is no conflict, the policy supplements the CBA.

PURPOSE:

The purpose of this policy is to define and document Employment Security Department's (ESD) Information Security requirements for the information technology (IT) functional areas. These areas are described in the Federal Information Security Management Act (FISMA), state, and Department information security program requirements.

POLICY:

Employment Security Department will ensure the implementation and documentation of agency:

- 1) Personnel information security controls as described in ESD Personnel Security Standard, 4201.
- 2) Physical and environmental protection controls as described in ESD Physical and Environmental Protection Standard, 4202.
- 3) Data security controls as described in ESD Data Security Standard, 4203.
- 4) Network security controls as described in ESD Network Security Standard, 4204.
- 5) Access security controls as described in ESD Access Security Standard, 4205.

- 6) Application security controls as described in ESD Application Development Security Standard, 4206.
- 7) Operations management controls as described in ESD Operations Management Security Standard, 4207.
- 8) Electronic commerce controls as described in ESD Electronic Commerce Security Standard, 4208.
- 9) Security monitoring and logging controls as described in ESD Security Monitoring and Logging Standard, 4209.
- 10) Incident response controls as described in ESD Incident Response Standard, 4210.

DEFINITIONS:

Controls - The management, operational, and technical objectives (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Personnel Security refers to controls designed to reduce risks associated with staff, business partner, or contractor use of technology resources. These risks include, but are not limited to, human error, theft, fraud, or misuse of information technology resources.

RELATED DOCUMENTATION:

1. Washington State Office of the Chief Information Officer
<http://ofm.wa.gov/ocio/policies/default.asp>
2. Washington State ISB Policy No. 401-S4:
http://isb.wa.gov/policies/401S_January2008version.doc
3. FISMA Security standards FIPS 199, FIPS 200, and NIST Special Publications 800-53, 800-59, and 800-60: <http://csrc.nist.gov/groups/SMA/fisma/index.html>
4. ESD Policy and Procedure 4100, "Information Security Governance"
5. ESD Information Security Governance Standard, 4101
6. ESD Information Security Governance Exception Procedure, 4101B
7. ESD Personnel Security Standards and Procedures, 4201
8. ESD Physical and Environmental Protection Standards and Procedures, 4202
9. ESD Data Security Standards and Procedures, 4203

10. ESD Network Security Standards and Procedures, 4204
11. ESD Access Security Standards and Procedures, 4205
12. ESD Application Security Standards and Procedures, 4206
13. ESD Operations Management Standards and Procedures, 4207
14. ESD Electronic Commerce Standards and Procedures, 4208
15. ESD Security Monitoring and Logging Standards and Procedures, 4209
16. ESD Incident Response Standards and Procedures, 4210

SUPERSEDES:

None

DIRECT INQUIRIES TO:

Information Technology Services Division
Brian Barta, [Information Security Manager](#),
(360) 407-4655