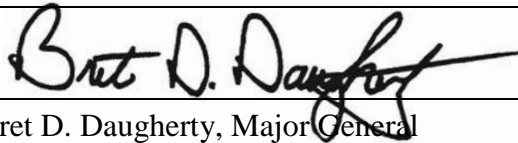




## Department Policy No. IT-302-04

|                               |   |
|-------------------------------|---|
| <b>Title:</b>                 | Information Technology Security   |
| <b>Former Number:</b>         | 00-027-04   |
| <b>Authorizing Source:</b>    | <a href="#">RCW 40.14 – Preservation and destruction of public records</a><br><a href="#">RCW 42.56.100 – Protection of public records – public access</a><br><a href="#">RCW 42.56.420 – Security</a><br><a href="#">RCW 42.56.590 – Notices of security breaches</a><br><a href="#">OCIO Policy 141 – Securing Information Technology Assets</a><br><a href="#">OCIO Policy 141.10 – Securing Information Technology Assets Standards</a><br><a href="#">Department Policy No. IT-306-05 – Use of State Provided IT Hardware and Software Resources</a> |
| <b>Information Contact:</b>   | Chief Information Officer<br>Building #20B (253) 512-7575   |
| <b>Effective Date:</b>        | May 28, 2004  |
| <b>Mandatory Review Date:</b> | January 13, 2020  |
| <b>Revised:</b>               | January 13, 2016  |
| <b>Approved By:</b>           | <br>Bret D. Daugherty, Major General<br>The Adjutant General<br>Washington Military Department Director   |

### Purpose

To establish a comprehensive Information Technology (IT) Security Program that reduces the risk of a network or data compromise and provides specific requirements and guidelines contained in the Washington Military Department (WMD) IT Security Program which ensure that the WMD is in compliance with the Office of the Chief Information Officer's (OCIO) Policy governing IT Security within the State of Washington.

## Scope

This policy applies to all WMD state and federal employees, contractors, vendors, and business partners who use IT systems connected to the WMD's "mil.wa.gov" network.

## Policy

### A. Responsibilities

1. Chief Information Officer (CIO) will:
  - a. Ensure that personnel assigned responsibilities defined in the agency IT Security Program are competent to perform the required tasks.
  - b. Ensure the necessary knowledge, skills, and abilities required for personnel performing work affecting the agency IT Security Program are documented.
  - c. Ensure that personnel assigned responsibilities defined in the agency IT Security Program must, at a minimum, receive training that addresses the OCIO Security Policy and Standard contained under OCIO IT Standards 2(5) and the agency's security policies and procedures.
2. IT Division Technical Staff will:
  - a. Ensure that appropriate scanning and monitoring tools, automated and manual, are employed on information systems to assess and monitor exploitable vulnerabilities, and insure policy adherence.
  - b. Review real-time and periodic audit logs including application & security logs along with web browsing history.
  - c. Coordinate with other WMD sections to ensure that this policy is implemented effectively.
  - d. Ensure that all contractors with access to Department IT Assets receive IT Security Orientation as required in OCIO IT Standard 2(1).
  - e. Ensure each Contractor is provided IT Security Orientation and a hard copy of the Department Policy No. IT-306-05: Use of State Provided IT Hardware and Software Resources. A record log will be kept by the ITSM reflecting the individual contractor's:
    - 1) Name
    - 2) Company
    - 3) Date of IT Security Orientation(s)
  - f. If it has been longer than 12 months since an individual contractor's last IT Security Orientation, they will be required to undergo a refresher IT Security Orientation in accordance with OCIO Standards 2(1).
  - g. Comply and ensure implementation of this policy and the WMD Information Technology Security Program within the WMD.
  - h. Manage and implement technologies that support the accepted WMD secure communication standards.

- i. Review periodically logging records to maintain compliance.
  - j. Document and report suspected intrusions, suspicious activities or unexplained erratic behaviors.
  - k. Collaborate with the IT Division Management Team to ensure a comprehensive solution or planned course of action is implemented.
3. WMD Division Directors will:
- a. Review the content of this policy and the WMD IT Security Program, and explain its importance in protecting the integrity of the WMD computing infrastructure with staff.
  - b. Require that all employees in their division take either the initial or annual refresher online IT Security Awareness training courses available through the [Washington State Learning Management System](#). The topics include the risks of data compromise, the employee's role in prevention, and how an employee can respond in the event their job function is affected by the incident.
  - c. Ensure new employees receive an overview of this policy prior to using the WMD computing infrastructure, computers, networks, and computer systems.
  - d. Review and recommend approval for exceptions to this policy.
  - e. Communicate all requests for exceptions to this policy to the WMD CIO.
  - f. Consider these questions before recommending approval for an exception to the policy:
    - 1) Is the requested exception really needed to perform the work of the agency?
    - 2) What risks would this exception create for the agency, the employee and yourself?
    - 3) What is the estimated impact on the WMD technology environment from this exception?
    - 4) What will it cost to implement and provide on-going support for this exception?
    - 5) Do you have the budget to accommodate the costs for this exception?
    - 6) What security risks does this exception generate?
4. Unit Managers, Supervisors and Employees:
- a. Each employee and contractor is responsible for the appropriate use of computing infrastructure, computers, networks and computer systems.
  - b. Supervisors are accountable for their employee's appropriate use of computing infrastructure, computers, networks and computer systems.
  - c. All employees understand that IT Security is the responsibility of everyone and not just IT Technical staff.