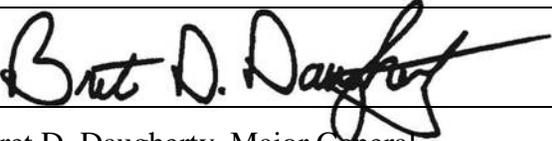




## Department Policy No. IT-311-18

<b>Title:</b>	Internet, Email, Electronic Records, and Computer System Policy Summaries; Employee Acknowledgement
<b>Former Number:</b>	DIR: Agency Computing and Network Environment
<b>Authorizing Source:</b>	<b>Washington State Rules and Regulations:</b> RCW 42.52: Ethics in public service WAC 292-110-010: Use of state resources <b>State of Washington Policies:</b> OCIO Policy No. 101: Technology Policies and Standards OCIO Standard No. 141.10: Securing Information Technology Assets <b>Washington Military Department Policies and Procedures:</b> <i>The Adjutant General</i> DIR-004-08: Public Records Disclosure DIR-005-08: Public Records Management DIR-005c-13: Email and Calendar Items <i>Information Technology</i> IT-302-04: Information Technology Security IT-306-05: Use of State Provided IT Hardware and Software Resources IT-307-05: Use of Mobile Telecommunications Devices TAG Directive: Remote Access of the Department Internet, Electronic Mail, and Computer Systems TAG Directive: Agency Computing and Network Environment IT-306-05: Use of State Provided IT Hardware and Software Resources <i>Unified Policies</i> 11-01: Social Media Policy
<b>Information Contact:</b>	Chief Information Officer Building #20B (253) 512-7575
<b>Effective Date:</b>	January 1, 2015
<b>Mandatory Review Date:</b>	May 23, 2022
<b>Revised:</b>	May 23, 2018
<b>Approved By:</b>	 Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

## Purpose

The purpose of this policy is to summarize the policies and laws that govern acceptable and legitimate uses of the Internet, electronic communications, IT hardware and software, and other technology resources at the Washington Military Department (WMD). Employees are required to carefully read each of the policies summarized and sign the attestation form provided as a condition of being granted permission to utilize WMD technology equipment.

## Scope

All WMD employees, contractors, consultants, temporaries, co-op students, and other workers accessing WMD systems on-site or remotely, and all systems and equipment that are owned or leased by WMD, including but not limited to, computer hardware (e.g., desktop computers, laptop computers, cellular telephones, tablets, and other physical media), software, operating systems, file transfer systems, networks, and all network user accounts providing access to document storage systems, electronic mail, and the Internet

## Policy

WMD is committed to protecting its employees, partners, and the agency from illegal or damaging actions by individuals, regardless of whether such actions are committed knowingly or unknowingly.

Effective, safe, and sensible use of technology is a collaborative effort involving the participation and support of every WMD employee and affiliate who deals with information technology and its related systems. It is the responsibility of every computer user to know the guidelines governing that technology and to conduct their activities accordingly. The rules detailed in the policies summarized by this document are in place to protect both the employee and the agency. Inappropriate use of technology resources exposes WMD to cyberattacks, compromise of network systems and services, ethical violations, legal liability and a host of other risks.

### A. State of Washington Statutes

1. [RCW 42.52 -Public Officers and Agencies; Ethics in Public Service.](#)

The Revised Code of Washington (RCW) Chapter 42.52 details the duties and responsibilities for those employed as public servants. Among other things, it defines 'state employee', 'agency', and 'official duty' and identifies activities that are incompatible with the proper discharge of the employee's duties.

2. [WAC 292-110-010 Agency Substantive Rules; Use of state resources.](#)

The Washington Administrative Code (WAC) 292-110-010 governs the use of state resources and is one that all state employees are responsible for following. It also states that agency employees may make an occasional, but limited, personal use of email or the Internet if (among other things) there is little or no cost to the state, the use is brief and infrequent, it does not interfere with the performance of the employee's official duties, and does not compromise the security or integrity of state property, information, or software. In addition to providing an overview of permitted uses, it reminds employees

that they have no expectation of privacy in electronic records generated using state resources. These provisions are also identified in the WMD's Ethics policy (HR-207-03).

## **B. State of Washington Policies**

### **1. [OCIO Policy No. 101: Technology Policies and Standards.](#)**

The Office of the Chief Information Officer (OCIO) published Policy No. 101 with the stated purpose of clarifying which institutions and agencies fall under its purview and to document the methods, roles, and responsibilities for developing and maintaining technology policy and standards. It specifies that all state agencies, as defined in RCW 43.41A.006, are subject to the policies issued by OCIO. This includes WMD.

### **2. [OCIO Standard No. 141.10: Securing Information Technology Assets.](#)**

OCIO Standard No. 141.10 sets the requirements for maintaining system and network security, data integrity, and confidentiality. It is commonly referred to as "141.10" by the IT Division and provides much of the driving force behind WMD technology policies. Agencies must ensure that personnel receive the proper education and training with respect to responsibilities associated with technology assets. The IT division is required to detail compliance with each component of this policy on an annual basis.

## **C. WMD Policies and Procedures**

### **1. *The Adjutant General***

#### **a) [DIR-004-08: Public Records Disclosure.](#)**

DIR-004-08 describes roles, responsibilities, and expectations for WMD employees with respect to public records disclosure. It defines what a public record under Washington State Law is and provides a summary of the Public Records Act (RCW 42.56, "the Act"). It also specifies what is required of WMD employees to remain compliant with the Act. This includes requirements for employees to be sufficiently knowledgeable about the Act, to assist the Public Records Officer in fulfillment of his/her duties, and to comply with all rules, regulations, and policies that govern public records.

#### **b) [DIR-005-08: Public Records Management.](#)**

The purpose of this policy is to ensure that WMD public records are preserved, stored, retained, transferred, destroyed, and disposed of cost-effectively in accordance with Washington State law, administrative codes, and Secretary of State Guidelines. It defines the distinct categories of information, clarifies record retention requirements, and provides a list of obligations for employees on how to properly handle the electronic records they create or have access to.

#### **c) [DIR-005c-13: Email and Calendar Items.](#)**

The purpose of this policy is to ensure that WMD email and calendar items are preserved, stored, retained, transferred, destroyed, and disposed of in accordance with Washington State law, administrative codes, and Secretary of State Guidelines. It also details the records retention requirements for email and calendar items.

## **2. Information Technology**

### **a) [IT-302-04: Information Technology Security.](#)**

This policy establishes a comprehensive IT Security Program that reduces the risk of a network or data compromise. It provides specific requirements and guidelines contained in the WMD IT Security Program to ensure that the WMD is in compliance with OCIO policies. It details the responsibilities of the IT Division, WMD management, and all other staff to ensure appropriate use of computing equipment.

### **b) [IT-306-05: Use of State Provided IT Hardware and Software Resources.](#)**

This policy establishes the WMD policy regarding employee use of State provided IT hardware and software resources and defines what constitutes inappropriate use. It identifies employees' roles and responsibilities, makes clear that employees do not have a privacy interest in the electronically stored information ("ESI") created during the course of their duties. Importantly, the Policy provides guidance and gives examples as to what are considered permissible and impermissible uses of WMD technology resources.

### **c) [IT-307-05: Use of Mobile Telecommunication Devices.](#)**

This policy establishes the WMD policies for assignment, use, and monitoring of state-issues mobile telecommunication devices, including cell phones, smartphones, air cards, satellite phones, and similar wireless access devices. Among other things, it reminds employees that physical security of the device is their responsibility and that all contents of the device including call, usage, billing, and data records; photos; and any personal data on the device are deemed as public records.

## **3. Unified Policies**

### **a) [11-01: Social Media Policy.](#)**

The purpose of this policy is to set clear guidelines and direction for the use of social media in the workplace. It identifies what constitutes permissible use of social media sites by WMD employees.

## Computer System Acceptable Use Agreement

I \_\_\_\_\_, have received, read, and agree to adhere to, each of the above referenced policies governing the appropriate use of technology and technology assets as a Washington Military Department (WMD) employee. Further, I understand that:

WMD IT systems are to be used in support of, and consistent with, the mission of WMD, the policies identified in Department Policy No. IT-311-18, and in relation to official state business.

Data and system logs created on agency systems remain the property of WMD and I have no ownership or privacy interest in such records and I have neither the right nor the ability to bar or prevent the disclosure of them.

WMD IT staff may monitor equipment, systems, Internet use, and network traffic at any time or when requested by management. This includes web browsing, email, and other activities incident to my use of state assets.

Hardware not owned or obtained by WMD may not be connected to the WMD network via wired, wireless, mobile hotspots, or any other type of access connection.

WMD will audit networks and systems on a periodic basis to ensure compliance with this and all other relevant policies.

I am responsible for ensuring my passwords are secure. I will not reveal my account password to others or allow use of my account by others.

I will not circumvent any security, privacy, or operations protocol, nor will I tamper with website blocking, user authentication, or other controls of any system, network, or account.

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

*Please return this form to the WMD Information Technology Division after signing. A copy of this form will be retained in your personnel file. If you have any questions as to the nature or content of this form, you may contact IT at 253-512-7111 or servicedesk@mil.wa.gov*