

MAINTAINING THE INFORMATION TECHNOLOGY SECURITY PROGRAM

Subject Matter Lead: Chief Technology Officer **Effective Date:** March 16, 2017

Accompanying Procedural Manual: PRO-IT-600A
Washington State Department of Agriculture
Information Technology Security Program **Accompanying
Forms:** N/A

Cancels: POL-IT-600, dated 6/25/2008

Sunset Review Date: July 2020

Approved By: *Derek I. Sandison*

References: OCIO POL-141.10 Securing Information Technology Assets Standards
RCW Chapter 39.34 Interlocal Cooperation Act

This policy, which applies to all agency employees and contractors, protects the integrity of agency data and the security of agency systems. It maintains privacy and prevents unauthorized access to data and systems.

1. THE IT SECURITY PROGRAM ADMINISTRATOR OVERSEES THE IT SECURITY PROGRAM

- The IT Security Program administrator annually updates the Information Technology Security Program document to meet Washington State Office of the Chief Information Officer Information Security Standards.
- The IT Security Program is independently audited every three years to comply with OCIO Security Program audit requirements.

2. THE DIRECTOR ANNUALLY SUBMITS WRITTEN CONFIRMATION TO OCIO THAT THE IT SECURITY PROGRAM IS IMPLEMENTED AND TESTED

3. PROGRAM MANAGERS ARE RESPONSIBLE FOR PROTECTING ACCESS TO THEIR PROGRAM'S DATA AND COMPUTER SYSTEMS

- Adequate controls and safeguards must be in place so that information on shared network drives is accessible only to those employees with a need for that information.
- Programs with sensitive information must secure access to information through appropriate file permissions.

4. ALL EMPLOYEES AND EXTERNAL CONTRACTORS MUST COMPLY WITH THE AGENCY'S IT SECURITY PROGRAM STANDARDS

- Employees and those with access to agency technology resources must receive annual security awareness training. Employees complete security awareness training when hired, and annually thereafter.
- Passwords are confidential and employees must not share them with anyone except IT Service Desk personnel.

5. INFORMATION STORED ON AGENCY COMPUTERS AND DEVICES IS THE PROPERTY OF THE AGENCY AND IS ACCESSIBLE, WITH OR WITHOUT NOTICE TO AN EMPLOYEE, FOR AUDITS, PROGRAM PURPOSES, PUBLIC RECORDS REQUESTS, OR TO INVESTIGATE SUSPECTED ABUSE.

6. DEVICES NOT OWNED BY THE AGENCY MAY NOT BE CONNECTED TO THE AGENCY-ADMINISTERED NETWORK OR TO ANY DEVICE SO CONNECTED, UNLESS APPROVED BY THE AGENCY CHIEF TECHNOLOGY OFFICER, WITH ONE EXCEPTION

- An example of a prohibited connection would be plugging a personally-owned laptop, a "thumb drive" flash memory device, or portable music player, into a computer attached to the State Government Network.
- Such non-state-owned devices may connect to the wireless network, "AGR-Guest," which is not attached to the State Government Network.
- The one exception is non-data-storing devices, such as printers. These may be connected to state-owned equipment under the following conditions:
 - The Chief Technology Officer or designee has approved the exception.
 - The employee has acknowledged in writing that liability for loss or damage to the device is not assumed by the state.

7. ALL EMPLOYEES MUST TAKE REASONABLE PRECAUTIONS TO KEEP VIRUSES AND OTHER UNAUTHORIZED SOFTWARE OFF AGENCY COMPUTERS

- IT Service Desk personnel will inform all users as to what software is authorized, instruct users in how to avoid inadvertently installing, and how to recognize the presence of, unauthorized software, and periodically scan computers and remove unauthorized software.
- Users may not download, open, execute or install software (including "shareware", public domain programs, software updates, or other executable files) unless all of the following conditions are met:
 - It has been approved by an IT Service Desk personnel.
 - It has not been identified as malware.
 - It is a supported and patched version, for security purposes.
 - It does not compromise system security or privacy.
 - It is not peer-to-peer file sharing application such as BitTorrent, Gnutella and Limewire.
 - It is not intended to circumvent security programs.

8. EMPLOYEES ARE RESPONSIBLE FOR REPORTING DAMAGE OR THEFT OF AGENCY TECHNOLOGY RESOURCES

- Virus and malware attacks must be immediately reported to IT Service Desk personnel.
- Computer equipment thefts must be reported to the Chief Technology Officer, Financial Services, and local police within 24 hours of discovering the loss. Copies of the complete police report should be sent to the Chief Technology Officer and Financial Services.
- Loss of classified information must be reported to the Chief Technology Officer and Administrative Regulations Manager by the next business day after discovering the loss.

9. EMPLOYEES WHO VIOLATE IT SECURITY POLICIES MAY BE SUBJECT TO DISCIPLINE, UP TO AND INCLUDING DISMISSAL

- Criminal sanctions resulting from illegal activities may also be applied by the appropriate court system.
- Managers must report all security incidents to their supervisor or the Chief Technology Officer.

DEFINITIONS:

Agency technology resources means all computing and telecommunications facilities, hardware, and software.

OCIO means Washington State Office of the Chief Information Officer.

IT means Information Technology.