Policy DOJ 7-74 Software Usage and Restrictions (CM-10/11)

Effective Date: *28 January 2020*
Reviewed Date: *January 3, 2023*
Applicability: *All Oregon Department of Justice regular, temporary, and volunteer employees, District Attorney Staff, and third parties under contractual obligations with the Agency.*
References: *ORS 276A.303, ORS 646A Oregon Consumer Identity Theft Protection Act; FISMA; NIST 800-53 rev 5; FBI CJIS Security Policy; IRS Publication 1075; OCSE FPLS; HHS Information Systems Security and Privacy Policy Automated Systems for Child Support Enforcement: A Guide for States; FERPA; CMS MARS-E; HIPAA; PCI-DSS; ACH; and DOJ Policy Manual.*

---

(1) Purpose

To establish the Oregon Department of Justice (Department) policy on software usage and restrictions and user-installed software to meet security and regulatory requirements.

(2) Scope

This policy applies to all Department employees, District Attorney Staff, contractors, vendors, and agents with an authorized computer system used to connect to the Department's technology systems. This policy applies to remote access connections used to do work on behalf of the Department, including reading or sending email and using intranet resources. This policy does not cover members of the public, who may have casual or incidental access to publicly accessible information or technology resources made available by the Department.

(3) Policy

The Department:

a. Develops, documents, and disseminates to all Department employees, District Attorney Staff, contractors, vendors, and agents with an authorized computer system used to connect to the Department technology resources:

1. A Software Usage and Restrictions policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the Software Usage and Restrictions policy and associated access controls; and

b. Reviews and updates the current:

1. Software Usage and Restrictions policy every three years (or if there is a significant change); and

2. Software Usage and Restrictions procedures at least annually.

Only software that is properly licensed, has a legal sufficiency review (if applicable), has a security review, and has been added to the Department's approved software list managed by Information Services for use may be installed on Department computer systems, including workstations and servers. This requirement also applies to open source, freeware, shareware, and demo software. Department approved and owned software cannot be installed on a personally owned computer without special approval.

All software procured by the Department is subject to the software publisher's license agreement. That agreement typically restricts how, and to whom, the software may be distributed. Department software purchasers, information services staff, employees/end users, and authorized individuals who approve the installation of software on a Department computer system must be knowledgeable of applicable license requirements and ensure that the use of the software will not violate any restrictions imposed by the software publisher, Oregon law, or Department rules or standards.

Department employees who purchase and install software must do so in accordance with this policy. Information Services must ensure that software acquired by and approved for installation on Department computer systems:

- Has the appropriate license(s);
- Is used in accordance with applicable licenses;
- Is appropriately documented with records of the software license(s); and
- Has been approved by management.

The requirements of this policy apply to existing as well as new or modified/enhanced software and software systems.

(4) Roles and Responsibilities

Roles and responsibilities related to DOJ Information Security are outlined in CIO Procedure 1-7.

It is the responsibility of all DOJ employees, District Attorney Staff, contractors, vendors, and agents to adhere to this policy and to refrain from any activity that might circumvent this policy.

The Information Security Officer shall:

- Perform a security review of software requested for use within DOJ.

Purchasing/Contracting Officers shall:

- Have contract oversight responsibilities and ensure that contractor-related security requirements are followed throughout the contract life cycle.
- Ensure that contractor employees have met the requirements detailed in Department

Procedure 7-75 Software Usage and Restrictions to receive access to Department systems and data.
- Purchase approved software only after a legal sufficiency and/or security review has been completed.

General Counsel Business Transactions Section shall:

- Perform a legal sufficiency review of software requested for use within the department based on ORS 291.047 and OAR 137-045-0010 through 0090
- Legal sufficiency reviews will be based on a minimum purchase price of $2500.00 or a perceived potential risk to the Department.
- Legal sufficiency will be for new software and upon renewal.

Department employees, information systems staff, and system administrators shall:

- Ensure that only software that is properly acquired and licensed by the Department is installed on department computer systems.
- Employees and authorized contractors and vendors must exercise common sense and good judgment in the use of Department computer systems and department approved software.
- Employees must safeguard, protect, and conserve department property and are responsible for the care, safety, and effective use of that property in accordance with this policy.
- Employees should report any misuse or unauthorized copying of software within the Department to their manager.

Violations of this policy are to be reported to the DOJ Information Security Officer by calling 503-378-5711 or by email using the "DOJInfoSec" email address in the Microsoft Outlook Global Address or DOJInfoSec@doj.state.or.us. Incidents may also be forwarded to DOJSIRT@doj.state.or.us.

(5) Definitions

For purposes of this policy:

Computer System: Any type of equipment that stores, processes, or transmits electronic data such as a server, desktop computer or laptops.

DOJ Approved: The Department holds an enterprise license to use the software or the CIO has approved the software for purchase or use on an DOJ computer system.

Software: Programs and applications that run on a computer, for example, word processors, spreadsheets, and databases. This policy is inclusive of all software applications including those that are original equipment manufacturer or 'bundled' software, freeware, shareware, and demo software.

Piracy: Illegal duplication of software for commercial or personal use. For purposes of this policy, "piracy" will also mean use of software that violates licensing restrictions and/or other misuse of the license agreement.

Pirated Software

Types of pirated software or licensing violations include:

Software that has been illegally copied Software that has been reproduced and/or distributed in violation of a software license Examples of pirated software include:

Counterfeit software: unauthorized copies of software created with the intent to directly imitate the copyrighted product. Counterfeit software is typically reproduced and distributed in a form to make the product appear legitimate and thus may include sophisticated efforts to replicate packaging, documentation, registration, logos, and security features.

Compilation Compact Discs (CDs): unauthorized copies of multiple software programs compiled onto a single CD. Compilation CDs typically include software programs published by a variety of software publishers.

Online pirated software: unauthorized copies of software distributed and downloaded via the Internet (including through peer-to-peer file sharing).

Other illegally copied software: software copied from disks, CDs, or other machines without authorization of the copyright owner.

(6) **Compliance**

Information Services and Procurement will review the authorized software list, policy, and process for obtaining software on a regular basis to ensure compliance.