Procedure DOJ 7-75 Software Usage and Restrictions (CM-10/11)

Effective Date: *January 28, 2020*
Reviewed Date: *January 3, 2023*
Applicability: *All Oregon Department of Justice regular, temporary, and volunteer employees, 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 describe the process the Oregon Department of Justice (Department) regular employees, temporary and volunteer employees, and authorized third parties who are issued DOJ computers or who access Department technology systems through authorized accounts must follow.

(2) Scope

This procedure is applicable to all Department approved software and the hardware using that software. Only the Attorney General or Deputy Attorney General can authorize the purchase or usage of software requiring an exception to Department policy.

(3) Software Usage and Restrictions Procedure

Information Services must establish procedures to ensure that all software purchased or acquired and installed on department computer systems adheres to the Department's Software Usage and Restrictions Policy. This includes purchased, freeware, shareware, open source, and demo/proof of concept software.

To avoid purchasing or installing unauthorized software, Information Services must ensure that:

- All software is properly licensed and approved for use on department computer systems, including Department owned workstations, laptops, mobile devices, and servers;
- Software purchases only occur from authorized contracted vendors/resellers or properly vetted sources (i.e., open source, freeware, and shareware);
- Software licenses are documented;
- A software record system that tracks the elements identified in Appendix E is maintained.

Employees should report any violations of the Software Usage and Restrictions Policy to Information Services and Procurement for review.

Questions regarding license requirements will be directed to the Department Procurement Team and Information Services.

(4) Roles and Responsibilities

The Chief Information Officer (CIO) is responsible for providing procedures, standards, and guidance to Department Executive Staff in support of the Department's Software Usage and Restrictions Policy, for managing software licenses. Software used by the Department must adhere to legal requirements set forth by the Deputy Attorney General.

Department Executives have the responsibility for ensuring that their divisions comply with the Software Usage and Restrictions Policy and Procedures.

The Deputy Attorney General sets the legal review thresholds for any licensed software.

General Counsel's Business Transactions Section has the responsibility for performing legal review of all software end user license agreements, terms of services agreements, and maintenance agreements, which includes both purchased software and open source/freeware, and shareware.

Information Services is responsible for:

- Establishing appropriate controls to prevent against unauthorized software installation;
- Deploying only approved software and software upgrades to department computer systems; and
- Auditing department computer systems to verify that unauthorized software has not been installed.

The Information Security Officer (ISO) is responsible for any security activities that pertain to Software Usage and Restrictions including security testing and examination of new software requests.

Department employees, temporary and volunteer employees, and authorized third parties will only use authorized software which has followed Department policy and procedure to obtain. Users will not install software, plug-ins, or miscellaneous applications without verification and approval that the software meets Department legal sufficiency, security review, and licensing requirements.

Appendix A
Software Request Workflow

See attached PDF document

Appendix B
General Counsel Business Transactions
Legal Sufficiency Software Review

The General Counsel Business Transactions Section (BTS) will perform a Legal Sufficiency review, based on ORS 291.047 and OAR 137-045-0010 through 0090, of the requested software.

Review will at a minimum cover the:

- Terms of Service
- End-user License Agreement

If required, BTS will engage the Software Vendor or their General Counsel to negotiate a rider or adjustment of licensing applicable to the Department. In the event a software vendor refuses to modify their EULA/TOS to meet Oregon requirements, the exception process must be followed. Only the Attorney General or Deputy Attorney General can authorize the purchase or usage of software requiring an exception to Department policy.

BTS will update the workflow ticket with an approval recommendation.

Appendix C
Information Security Review

As part of workflow, the Department's Information Security Team will test the requested software. Process will incorporate 32 calendar days for testing that includes 1-day administrative setup and 31 days continuous testing and monitoring.

Testing setup will be on a standalone platform not connected to the Department's secure network.

- A computer system, with sufficient resources, for hosting virtual machines (VM) to test requested software.
- Native Microsoft Hyper-V for the virtual environment.
- Host will be provisioned to allow multiple connections to the internet through a standalone connection circuit (the Department currently uses DSL).
- Host provisioned with packet capture capability to monitor network traffic to and from the VM.
- Installation activity monitored and logged for review.

DOJ Information Security will:

- Look for attempts by software to "Call Home".
- Review what registry entries are made.
- Review what files are copied to the computer system.
- Review what accounts are created or any indication of privilege escalation.
- Review any National Vulnerability Database entries for the requested software.
- Review industry forum entries for the requested software indicating vulnerabilities (i.e., a zero day).
- Review the available privacy policy for the software and vendor.
- Update the workflow ticket with the results and an approval recommendation.

Appendix D
Mobile device application/software testing

Using the same procedures outlined in Appendix C perform testing on mobile device application.

Using the testing platform described in Appendix C, a review will be conducted by connecting a test mobile device through wireless to the device to utilize the packet capture capabilities.

The Department's Information Security Team will test for current iOS and Android applications.

Appendix E
Department Information Services Software Tracking

Maintain an Approved Software list with the following data elements at a minimum:

- Type (SaaS, COTS (Network/Desktop)
- Description of Application
- License type
- Availability (for per user or machine licenses)
- License Type
- Contract or Price Agreement
- BTS Review
- BTS Review Date
- Security Review
- Security Review Date
- Vendor Website or DOJ Site
- Maintain copy of software licensed or current stable version otherwise.

Information Services will additionally:

- Manage all approved software for installation and do so using the concept of least privilege and least functionality.
- Ensure all approved software that has been installed is up to date and patched.
- Remove end-of-life or end-of-support software from use as it is a security risk.
    - If an end-of-life or end-of-support software cannot be removed an exception will be submitted, reviewed, and approved on a case by case basis. The exception must include a plan for replacing, upgrading, or removing in a specified timeline the end-of-life or end-of-support software.