Curry County Vendor Security Questionnaire

Version 1.0 – October 2025

Curry County Oregon
Information Technology Department
94235 Moore Street, Suite 125
Gold Beach, OR 97444
Phone: (541) 247-3371
Email: TechStop@CurryCountyOR.gov

This security questionnaire is intended to evaluate vendor security policies and practices in conjunction with Curry County's vendor evaluation and procurement processes. Your candid and timely responses will help us determine the cybersecurity posture of vendors providing software, hardware, or services to the County.

Please answer "N/A" for non-applicable questions or "Unknown" if you are not certain of the answer.

1.1 AUTHORITY

This document is designed to align with Curry County Information Technology policies, Oregon state law, and relevant federal regulations and standards. Applicable references include but are not limited to the following:

Federal Laws & Directives

- NDAA Section 889, EO 13873/13942/13943/13971, FAR 52.204-23–26 – Banned hardware, software, and services.
- Executive Order 14028 – Improving the Nation's Cybersecurity.
- Executive Order 14117 – Preventing Access to Americans' Bulk Sensitive Personal Data.
- Executive Memoranda M-21-07, M-21-30, M-22-09 – IPv6 transition, critical software protection, and Zero Trust principles.
- DOJ 21-971 – Civil Cyber-Fraud Initiative.
- DHS/CISA Binding Operational Directive 22-01.
- U.S. National Cybersecurity Strategy (2023).

Oregon Laws & Frameworks

- ORS 646A.600 – Oregon Identity Theft Protection Act.
- ORS 646A.604 – Notice of Breach of Security.
- ORS 192.553 – Protected Health Information.

- ORS 276A.300–320 – Cybersecurity Coordination and OSCIO Authority.
- Oregon Statewide Information Security Plan.

Data and Compliance Standards
- HIPAA – Health Insurance Portability and Accountability Act.
- IRS 1075 – Tax Information Security Guidelines.
- PCI DSS – Payment Card Industry Data Security Standard.
- CJIS Security Addendum and Contractor Policies (CJIS CA-3, PS-3, SC-28, IR-6, SI-2).
- NIST SP 800-53, SP 800-161r1, and NIST Cybersecurity Framework (CSF 2.0).
- CIS Controls, CMMC, and Cloud Security Alliance CCM.

---

2. QUESTIONS

Section I – Administrative
1. How do you inform customers about security issues?
2. How long do you wait to inform customers of a security issue?
3. What cybersecurity or industry frameworks, if any, is your organization officially aligned with (e.g., NIST 800-53 Moderate)?
4. Has your organization engaged independent third parties to perform information security audits and/or risk assessments in the last two years?
5. If your operations meet the definition of a "service organization" per SSAE 18, can you provide a copy of your latest SOC 1 (Type I or Type II, as applicable) or SOC 2 report?
6. Do you have dedicated cybersecurity staff and a CISO?
7. Do you have any internal security questionnaire forms or external attestations completed and available for your customers that you can provide for us? Examples of questionnaires would include SIG LITE, VSA or CSA CAIQ. Examples of attestations would include ISO 27k or SOC.
8. Are you familiar with Curry County's Incident Response and Reporting Procedures?

Section II – Qualifications and Staffing
1. How many years has your organization provided the product or services requested in this RFP?
2. When do you conduct background checks on your employees, and what is included (e.g., criminal, drug testing, credit)?
3. What measures do you take to ensure your staff maintains confidentiality of customer data?
4. How often is compliance and security training provided for your staff?
5. Would your organization be able to provide a full or partial Software Bill of Materials (SBOM)? For example: Log4J 2.17, SQL Server Express 2019, 7zip 21.06.

6. Would your organization be able to provide a full or partial Behavioral Transparency Manifest (list of domains, IPs, or ports that your software accesses, or local files it touches)?
7. Are your staff who may have access to Curry County data required to complete CJIS background and security training?

Section III – Data
1. Will this product or service generate, store, or transmit data containing PII, CJIS, PHI, PCI, or any protected, sensitive, or controlled unclassified information (CUI)?
2. Does your organization fully adhere to the legal requirements for the given data classification (e.g., PCI compliance for PCI data, HIPAA compliance for HIPAA data)?
3. Where is the data stored (geographically and by provider)?
4. Who owns the data?
5. Is the data encrypted at rest?
6. Is the data encrypted in transit?
7. What happens to the data if the partnership ends?
8. Will any third party have access to our data? If yes, identify them.
9. Who is responsible for data recovery in the event of a data loss?
10. Confirm that all data related to Curry County is stored within the United States unless otherwise approved in writing.

Section IV – Technical
1. How frequently is the product software / firmware updated, and what is the update process?
2. Do you use any hardware, software, services, or support from manufacturers banned by the U.S. Government (see NDAA Section 889)?
3. Does your service, hardware, or software support Internet Protocol version 6 (IPv6) and have full feature parity with IPv4 as mandated by OMB M-21-07?
4. What antivirus exceptions, firewall exceptions, or other security exceptions are required for your product or service to function?
5. Do any of your staff share accounts or passwords for logging in? If so, are shared account passwords changed every time an employee leaves?
6. Do you require remote access to our network or product/device on our network? If so, what systems and services do you typically use for this remote access?
7. What files or other data does your product or service send outside of our local network (e.g., telemetry, license usage/verification)?
8. Do you require MFA for your staff accounts?
9. Does your product or service ship with or include any known vulnerabilities or vulnerable components more than 90 days past a vendor patch being available?
10. Were known vulnerable systems or services used in the building, deployment, or

delivery of this product or service?
11. Does your product require MFA for customers?
12. Does your product support Single Sign-On (SSO)? (e.g., OIDC or SAML integration with Entra ID.)

Section V – Practices
1. Does your product or service require the use of any known-insecure or deprecated practices? If yes, please provide details. Examples include:
- Default credentials that do not require reset on first login.
- Passwords that are identical across clients.
- Network shares of existing OS-created folders (e.g., C:\).
- Requirement to use unsupported OS or software (e.g., VB6, .Net 2.0, Java 6).
- Requirement of insecure protocols (e.g., SMB1, telnet, TLS 1.1).
- Requirement to disable OS patching or security updates.
- Use of deprecated or known-vulnerable third-party software (e.g., Log4J 1.x, PHP 7.2).
- Executable content that is not digitally signed.
- Requirement for all users to be local administrators.
- Hard-coded encryption keys, salts, or secrets that are not unique per client.
- Storage of passwords in plain text or encrypted rather than hashed.

Section VI – Acknowledgment
By signing below, the vendor confirms that the responses provided are accurate to the best of their knowledge and that they agree to comply with Curry County's cybersecurity, data protection, and reporting policies.

Vendor Company Name: _____
Vendor Representative (Print): _____
Signature: _____ Date: _____
Title: _____
Phone/Email: _____

Curry County IT Reviewer: _____
Date Reviewed: _____

Questions?
Contact the Curry County IT Department at TechStop@CurryCountyOR.gov or (541) 247-3371.

End of Document – Curry County Vendor Security Questionnaire v1.0 (October 2025)