



Security Questionnaire

Created Date:	Oct. 1, 2024
Last Update:	Feb. 3, 2026
Version:	2

Introduction

To enhance our understanding of your organization's software security practices and ensure alignment with industry standards, OntarioMD requests that vendors complete the following questionnaire.

This assessment is designed to evaluate the security compliance of software suppliers serving Ontario's healthcare sector. The questions contained within this document are derived from the Canadian Centre for Cybersecurity's comprehensive guidelines, providing a robust framework for assessing your organization's security posture. More information can be found at the following link:

<https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071>

Questionnaire

For each of the following questions, answer with either Yes or No. If your answer is “No”, please provide a detailed explanation to clarify your selection and provide additional context in the Comments field. For select questions, additional comments will be requested.

Date of Submission (Required): Click or tap to enter a date

Vendor Name: _____

1. Are you using a secure software development lifecycle (SSDL) framework and is it documented?	Choose an item.
Comments:	
2. Do you have a documented process to prove that the activities described in the SSDL occur as expected?	Choose an item.
Comments:	
3. Do you incorporate security practices at every stage of the software development lifecycle?	Choose an item.
Please outline the security practices in the comments below.	
Comments:	

4. Are strong security standards and controls applied at every stage of the development lifecycle to monitor and manage the production processes?	Choose an item.
Comments:	
5. Do you have a fulltime knowledgeable software security team?	Choose an item.
Comments:	
6. Are your team members educated on secure software development, open-source security, and DevSecOps practices?	Choose an item.
Comments:	
7. Do you perform employee background checks?	Choose an item.
Please outline the frequency in the comments below.	
Comments:	
8. Do you only use developers who keep detailed records of the dependencies used in their software? Are the developers keeping up to date with the latest versions of their library dependencies?	Choose an item.
Comments:	
9. Is the mitigation of known vulnerabilities factored into product design?	Choose an item.
Comments:	
10. Are you staying current on new evolving vulnerabilities? Do you get alerted to vulnerability disclosures?	Choose an item.
Comments:	

11. Do you have a well-documented system for patching security flaws and fixing security defects?	Choose an item.
Comments:	
12. Are vulnerabilities actively identified and disclosed? Do you have a vulnerability response program and team in place?	Choose an item.
Comments:	
13. Are your software security activities and products reviewed by a third-party?	Choose an item.
Comments:	
14. Do you have a software configuration management (SCM) process in place to track, manage, and control the changes in the software/codes during the software development lifecycle?	Choose an item.
Please provide more details of this process in the comments below.	
Comments:	
15. Can you ensure that your organization's data will be protected? Do you use data encryption, and do you dispose of the data when the relationship with their clients is completed?	Choose an item.
Please disclose the type of encryption used along with how data is securely disposed of.	
Comments:	
16. Do you have internal auditing procedures for all your security operations?	Choose an item.
Comments:	
17. Can you confirm software integrity by using a code authentication mechanism?	Choose an item.
Comments:	

18. Do you have a software component inventory or a software bill of material (SBOM) to track components, and audit your controls to keep software secure? What details are included in the SBOM?	Choose an item.
Comments:	

19. Do you have protocols for how to notify appropriate stakeholders in the event of a breach?	Choose an item.
Comments:	