**Security Requirements for WebMethods Retirement Project V1**

As of May 16, 2022

This document is intended to outline what security requirements ISB requires during development mode as well as once in operational/maintenance mode.

**PART 1: Mandatory Security Protocols during development mode and before production delivery are**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ITEM** | **DESCRIPTION** | **ACTIONS REQUIRED** | **RECOMMENDED TOOL** | **LINK TO MORE INFORMATION** |
| **Static scanning**  **(scans code that isn't running)** | Scan of code before it runs and supporting libraries. | On build or on deployment AND Recurring monthly scan and review and action of high and or critical against OCIO patching guidelines. | SonarQube, CodeQL, Dependabot | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations)    [OCIO Patch Guidelines](https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/defensible-security/ocio_patch_guidelines_-_2021-02-18.pdf)  <https://github.com/dependabot> |
| **Dynamic Scanning** | Tests against running/live code | On every build or on deployment prior to production   * For OWASP ZAP   + Use the ‘full scan’ feature.   + Any resulting ‘high’ results MUST not be promoted to production. | OWASP ZAP | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations) |
| **Container image scanning (active)** | Scans against the components of the code that active to ensure up to date and not vulnerable | Request scan recurring frequency; Monthly at a minimum    Following up at least once a month of going live and remediate medium, high, critical vulnerabilities as they are found against OCIO patching guidelines | Aqua | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations) |
| **Image storage and Container image scanning (active)** | Tool to scan the components of the code | For every image deployed to production | BC Government's Artifactory | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations)    [Artifactory](https://developer.gov.bc.ca/Artifact-Repositories-(Artifactory)) |
| **Secrets management** | Best practices for managing credentials | All secrets should be managed through the BC Governments ‘VAULT’ instance. Ensure secrets and or any credentials aren’t exposed as plaintext in application or repository. | [BC Gov's Vault instance](https://developer.gov.bc.ca/BC-Government-Vault-Secrets-Management)  or provincially provided equivalent | [BC Government OpenShift DevOps Security Consideration Access Management](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations#htmlheadheadbodya-nameaccess-managementabodyhtmlhtmlheadheadbodybodyhtmlaccess-management) |
| **Pipeline Tools** | Allows for consistent and repeatable deployments of code which include scanning tools | On every build and deployment have a pipeline tool and template.  No critical vulnerabilities or code that is or has reached End of Life (EOL) will be promoted to production. | * + [Tekton Templates](https://github.com/bcgov/pipeline-templates/tree/main/tekton)   + [Github Templates](https://github.com/bcgov/pipeline-templates/blob/main/docs/github.md)   + [ZAP Scanning Report](https://github.com/bcgov/security-pipeline-templates/blob/zap-scan/README.md) | <https://github.com/bcgov/pipeline-templates> |
| **Image Tagging** | Tagging allows for management of code and reduces time to deploy in the case of a vulnerability | Ensure image tagging is applied to image stream. Recommended   |  |  | | --- | --- | | **Description** | **Example** | | Revision | myimage:v2.0.1 | | Architecture | myimage:v2.0-x86\_64 | | Base image | myimage:v1.2-centos7 | | Latest (potentially unstable) | myimage:latest | | Latest stable | myimage:stable |   *Table 1. Image Tag Naming Conventions.* From <[*https://docs.openshift.com/container-platform/3.11/dev\_guide/managing\_images.html*](https://docs.openshift.com/container-platform/3.11/dev_guide/managing_images.html)> | n/a | <https://docs.openshift.com/container-platform/3.11/dev_guide/managing_images.html>    <https://developer.gov.bc.ca/Developer-Tools/Best-practices-for-managing-image-streams> |
| **Logging** | Logging allows for teams to support any provincial investigations and align to the province’s standard | * Ensure that Personal Identifiable information (PII) is not logged or is parameterized * Ensure logs are accessible for 90 days for application. Examples of levels of logs: Application, DNS, Ingress, Egress, Route, Service, pod(s) and access logs * SHOULD not use GET requests for logging with PII | BC Government's Kibana instance or provincial provided equivalent, AG Splunk instance. | [Information Security Classification Standards](https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/information_security_classification_standard_july_17_2018.pdf) |
| **Repository management** | Allows for code provided from teams to be centrally | Must use GitHub's BC Gov organization:   * bcgov - main developer git repository for platform application code and/or public sharing. * bcgov-c - main private git repository used for cluster configuration management and non-public projects. * bcdevops - alternate git repository for platform application code. Membership required for access to OpenShift. * bcgov-platform-services - git repository for platform services team |  | <https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations> |
| **Dependency management** | Automated dependency updates built into GitHub | The following need to be always enabled for the lifecycle of this application   * Dependabot alerts * Dependabot security updates     Pull requests should FAIL and not be promoted to production on 'any' or 'high or higher' vulnerabilities found in dependabot. Dependabot alerts MUST be actioned against OCIO Patch Guidelines | Dependabot for the code  <https://github.com/dependabot> | <https://docs.github.com/en/code-security/dependabot/dependabot-security-updates/configuring-dependabot-security-updates> |
| **API Management** | Best practices for teams to manage modern technology in making requests to pass data or requests. | Follow ' **API Security Top 10 2019** From <<https://owasp.org/www-project-api-security/>> ' |  | [Information Security Standards](https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/security_standard_application_web_development_deployment.pdf)  [BC Government API Guidelines](https://developer.gov.bc.ca/BC-Government-API-Guidelines)  [REST Security Cheat Sheet](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/REST_Security_Cheat_Sheet.md) |

**PART 2: Mandatory Security Protocols during operational support or maintenance mode are:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ITEM** | **Description** | **Actions** | **Recommended Tool** | **Link to Process** |
| **Container Image Scanning** | Scans against the components of the code that active to ensure up to date and not vulnerable | This scanning must be completed within 1 month of going live. Any vulnerabilities must be identified, and remediate medium, high, critical vulnerabilities as they are found against OCIO patching guidelines | XRay Trivy | <https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations> |
| **Certificate Management (TLS)** | Best practices for managing certificates that align to Government of BC security standards | Ensure there is support and coverage for certificate management, deployment, and maintenance at least on an annual basis or certificate renewal (yearly or every 3 years) | n/a | <https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations>  <https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/cryptographic_standards_v17.pdf> |
| **Branch management within GitHub** | Best practices for management of code and access to ensure integrity of the data | * Allow for branch protected * Disable force pushes to branches * Review and have an approver for Pull Requests (PR) before merging * Don’t change the defaults for branch deletion (do not allow for deletion of branches without 2nd approval) | n/a | <https://docs.github.com/en/repositories/configuring-branches-and-merges-in-your-repository/defining-the-mergeability-of-pull-requests/about-protected-branches#include-administrators> |
| **Static scanning**  **(Scans code that isn't running)** | Scan of code before it runs and supporting libraries. | On build or on deployment AND Recurring monthly review and action of high and or critical against OCIO patching guidelines. | SonarQube, CodeQL, Dependabot | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations)    [OCIO Patch Guidelines](https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/defensible-security/ocio_patch_guidelines_-_2021-02-18.pdf) |
| **Dynamic Scanning** | Tests against running/live code | On every build or on deployment prior to production  For OWASP ZAP   * Use the ‘full scan’ feature. * Any resulting ‘high’ results MUST not be promoted to production. | OWASP ZAP | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations) |
| **Container image scanning (active)** | Scans against the components of the code that active to ensure up to date and not vulnerable | Request scan recurring frequency; Monthly at a minimum.    Following up at least once a month of going live and remediate medium, high, critical vulnerabilities as they are found against OCIO patching guidelines | Aqua or XRay; recommend XRay. | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations) |
| **Image storage and Container image scanning (active)** | Tool to scan the components of the code | For every image deployed to production | BC Government's Artifactory | [BC Government OpenShift DevOps Security Considerations](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations)    [Artifactory](https://developer.gov.bc.ca/Artifact-Repositories-(Artifactory)) |
| **Secrets management** | Best practices for managing credentials | All secrets should be managed through the BC Governments ‘VAULT’ instance.  Ensure secrets and or any credentials aren’t exposed as plaintext in application or repository. | [BC Gov's Vault instance](https://developer.gov.bc.ca/BC-Government-Vault-Secrets-Management)  or provincially provided equivalent | [BC Government OpenShift DevOps Security Consideration Access Management](https://developer.gov.bc.ca/BC-Government-OpenShift-DevOps-Security-Considerations#htmlheadheadbodya-nameaccess-managementabodyhtmlhtmlheadheadbodybodyhtmlaccess-management) |
| **Pipeline Tools** | Allows for consistent and repeatable deployments of code which include scanning tools | On every build and deployment have a pipeline tool and template.No critical vulnerabilities or code that is or has reached End of Life (EOL) will be promoted to production. | * [Tekton Templates](https://github.com/bcgov/pipeline-templates/tree/main/tekton) * [GitHub Templates](https://github.com/bcgov/pipeline-templates/blob/main/docs/github.md) * [ZAP Scanning Report](https://github.com/bcgov/security-pipeline-templates/blob/zap-scan/README.md) | <https://github.com/bcgov/pipeline-templates> |
| **Image Tagging** | Tagging allows for management of code and reduces time to deploy in the case of a vulnerability | Ensure image tagging is applied to image stream. Recommended   |  |  | | --- | --- | | **Description** | **Example** | | Revision | myimage:v2.0.1 | | Architecture | myimage:v2.0-x86\_64 | | Base image | myimage:v1.2-centos7 | | Latest (potentially unstable) | myimage:latest | | Latest stable | myimage:stable |   *Table 1. Image Tag Naming Conventions.* From <[*https://docs.openshift.com/container-platform/3.11/dev\_guide/managing\_images.html*](https://docs.openshift.com/container-platform/3.11/dev_guide/managing_images.html)> | n/a | <https://docs.openshift.com/container-platform/3.11/dev_guide/managing_images.html>    <https://developer.gov.bc.ca/Developer-Tools/Best-practices-for-managing-image-streams> |
| **Logging** | Logging allows for teams to support any provincial investigations and align to the province’s standard | * Ensure that Personal Identifiable information (PII) is not logged or is parameterized * Ensure logs are accessible for 90 days for application. Examples of levels of logs: Application, DNS, Ingress, Egress, Route, Service, pod(s) and access logs * SHOULD not use GET requests for logging with PII | BC Government's Kibana instance or provincial provided equivalent, AG Splunk instance. | [Information Security Classification Standards](https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/information_security_classification_standard_july_17_2018.pdf) |
| **Dependency management** | Automated dependency updates built into GitHub’ | The following need to be enabled at all times for the lifecycle of this application   * Dependabot alerts * Dependabot security updates     Pull requests should FAIL and not be promoted to production on 'any' or 'high or higher' vulnerabilities found in dependabot  Dependabot alerts MUST be actioned against OCIO Patch Guidelines | Dependabot for the code <https://github.com/dependabot> | <https://github.com/dependabot>  <https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/defensible-security/ocio_patch_guidelines_-_2021-02-18.pdf> |