Portfolio++™ Security
Version 1.3
Last Updated: July 11, 2024

Table of Contents:

1. Introduction

This document outlines the security measures and recommended protocols to help ensure data privacy when using Portfolio++™.

Portfolio++™ is a software extension to Azure DevOps. Portfolio++™ is installed in an end-user's on-premise Azure DevOps Server, or hosted in Microsoft Azure Cloud Services.

The document is focused on three roles: Client-User, Client-Administrator, and Vendor-Software.

2. Security Responsibilities

2.1 Client-User

As a User of Portfolio++™, you are responsible for:

- Secure Authentication: Portfolio++™ requires that you be authenticated through your Microsoft login ID, and in turn, that you have access to Azure DevOps. Ensuring that your Microsoft login credentials use strong and unique passwords is strongly recommended. We recommend the use of Microsoft Authenticator.
- Data Visibility: Portfolio++™ adheres to each user's Azure DevOps Project/Team visibility settings, as set for them in Azure DevOps, by the Azure DevOps Administrator.
- Incident Reporting: Promptly report any security incidents or vulnerabilities to your Azure DevOps Administrators.

2.2 Client-Administrator (Azure DevOps)

As an Administrator of an environment running Portfolio++™, you are responsible for:

- Access Control: Managing User access and permissions, including granting and revoking access to projects. We also recommend that Administrator's only provide users with access to Projects/Data in Azure DevOps, **only when it is necessary**, i.e., adhering to the principle of least privilege.

- Security Configuration: Configuring Azure DevOps security settings to ensure data protection and compliance sufficient to the needs of your organization.
- Incident Response: Developing and implementing security breach incident response procedures, including notification of the hosting company.
- Regular Audits: Conducting regular security audits and assessments to identify and mitigate potential vulnerabilities to Azure, and your Azure DevOps Organizations.

2.3 Vendor-Software (Portfolio++™)

The Vendor is responsible for:

- Network Security: implement and maintain network security measures that protects the software and safeguards sensitive data using encryption both during transmission and at rest.
- API Security: ensuring security, integrity, and user access control measures are in place for the Portfolio++™ Pro Subscription Validation API that resides in the Vendor's environment.
- Compliance: ensuring that their infrastructure complies with regulations and standards.

3. Access Control

3.1 User Access to Azure DevOps Data

When Portfolio++™ is installed into an Azure DevOps Organization, the data that is retrieved for a user is based on that's user's Azure DevOps access permissions, as set by the Azure DevOps Organization Administrator. As such, Portfolio++™ only provides access to Azure DevOps Projects that the Administrator has granted the user permission to access.

3.2 Administrator Azure DevOps Controls

Administrators have the authority to manage user access to Azure DevOps and its Projects. They can grant access to new Users, modify permissions for existing Users, and revoke access when necessary. Administrators are responsible for ensuring that access is granted based on the principle of least privilege.

3.3 Access Revocation in Azure DevOps

Access to projects can be revoked by Administrators at any time. This may occur when a user no longer requires access to a project or when a user's permissions need to be modified. When access is revoked, the user will no longer be able to view or interact with the project.

3.4 Audit Logging

All access requests, approvals, and revocations are logged for auditing purposes in Azure DevOps. Administrators can review these logs to ensure that access is being managed appropriately and to identify any potential security issues.

4. Incident Response

4.1 Incident Reporting

Users and Administrators are encouraged to report any security incidents or vulnerabilities suspected to be related to Portfolio++™ use promptly. Reports can be submitted by emailing info@itrellis.com and should include a description of the incident and any relevant details.

4.2 Incident Classification

Upon receiving a report of a security incident, the incident response team will classify the incident based on its severity and impact. This classification will determine the urgency and level of response required. All incidents reported will be acknowledged within 24 hours.

4.3 Incident Response Plan

An incident response plan has been developed to guide the Portfolio++™ incident response to security incidents. The plan outlines the steps to be taken in the event of an incident, including notifying affected Users, containing the incident, and mitigating any potential damage.

4.4 Incident Resolution

The incident response team will work to resolve the incident in a timely manner. This may involve taking the affected system offline, applying patches or updates, or implementing other remediation measures.

4.5 Communication

Regular updates will be provided to affected Users and stakeholders throughout the incident response process. Communication will be transparent and timely, with the goal of keeping everyone informed of the situation and the steps being taken to resolve it.

4.6 Post-Incident Review

After the incident has been resolved, a post-incident review will be conducted to assess the response and identify any areas for improvement. Lessons learned from the incident will be used to update and improve the incident response plan for future incidents.

5. Compliance

5.1 Regulatory Compliance

iTrellis complies with General Data Protection Regulation ("GDPR") where applicable. The Portfolio++™ development team ensures that their infrastructure and development practices meet the requirements of these regulations and standards.

5.2 Data Privacy

iTrellis is committed to protecting the privacy of user data. Personal data is collected, processed, and stored in accordance with applicable data protection laws and regulations. Our Data Privacy statement is published here: https://www.itrellis.com/data-privacy

5.3 Security Audits

Regular security audits are conducted to assess the security of Portfolio++™. These audits help to identify and mitigate potential vulnerabilities, ensuring that the software remains secure and compliant with relevant regulations.

5.4 Compliance Reporting

iTrellis provides compliance reports to Users and stakeholders upon request. These compliance reports details tests that are run routinely, and ensure that API endpoints, data stores, network access, etc. are protected.

5.5 Continuous Improvement

iTrellis is committed to continuous improvement in security and compliance. Feedback from audits, incidents, and user input is used to improve security measures and ensure ongoing compliance with regulations and standards.