PHOENIX

Phoenix Secure Coding Guidelines

PHX041

Contents

1. Document Control

1.1 Purpose of this guide

This document establishes the Secure Application Development Code standards and guidelines, this document establishes the minimum practices to ensure secure code is developed and implemented on systems developed within the Phoenix Systems Development Team and excludes the License Dashboard Development Team.

Developers must consider security as an integral part of their role.

These top 5 most common vulnerabilities are a direct result of inadequate secure coding practices:

- Cross-Site Scripting
- SQL Injection
- HTTP Response Splitting
- Content Spoofing
- Information Leakage

1.2 Scope

This document applies to all members of staff that perform development of systems owned the Phoenix Systems Development Team and excludes the License Dashboard Development Team.

2. Policy

The adherence to and use of the Secure Code Guideline document is a requirement for all software development on Phoenix Software Ltd information technology systems

All code developers shall verify that their code is in compliance with the most recent and approved coding standards and guidelines.

Only validated code shall be implemented into the company's production environment.

A review and validation ensures that code exhibits fundamental security properties to include correctness, predictability and attack tolerance.

2.1 Security in the software development lifecycle

It is paramount that security requirements are identified throughout the development lifecycle. Application Code Developers shall:

- ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle

- ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended
- never trust incoming data to the system, apply checks to this data
- never rely on the client to store sensitive data no matter how trivial
- disable error messages that return any information to the user
- applications must validate input to ensure it is well-formed and meaningful
- personal data is only available to the relevant people in accordance to the data protection act
- credit card information and logins are all encrypted
- all web applications consider the item detailed in OWASP Top 10-2017
- ensure a code review in undertaken for any areas of development pertaining to the points listed above

2.2 Security of the development environment

Access to the Phoenix Software Azure DevOps organisation is restricted to members of the development team and certain key internal stakeholders. Access is further restricted via Azure DevOps group membership to project administrators, project team members, and stakeholders.

Who has access and their level of access is periodically reviewed.

2.3 Security guidelines for Oasis v3 Development

Access to client applications for Oasis are determined by Active Directory group membership. All users of Oasis need to be a member of one of the following groups:

- Oasis_AccountManager – enables processing of sales order and access to the sales application
- Oasis_CreditController – enables access to the credit control application
- Oasis_CreditControllerManager – enables access to management functions in the credit control application
- Oasis_CustomerServiceAgent – enables access to the customer service application
- Oasis_DispatchClerk – enable access to the Despatch application
- Oasis_ExecutiveManager – enables access to the Management Accounts application
- Oasis_Marketer – enables access to the marketing application
- Oasis_SalesAdministrator – enables access to the sales application
- Oasis_SalesManager – enables access to management functions in the sales application
- Oasis_UberDeveloper – enables unlimited access to all Oasis applications
- Oasis_Consultant – enables access to the Service Desk application
- Oasis_ConsultantManager – enables access to management functions in the Service Desk application
- Oasis_Operations – enables access to the Operations application
- Oasis_OperationsManager – enables access to management functions in the Operations application

There are equivalent active directory groups for systems testing and user acceptance testing these are prefixed with TestOasis_ instead of Oasis_.

Non-production environments of Oasis must have the Is Live property set to False in the web.config of the WCF Service. This ensures that all emails generated by the system are sent to a test email address, and that all Sage integration uses the test Sage environment.

Versions of new production systems for Oasis need to be authorised by the Development Manager or Operations Director before they can be deployed.

2.4 Security guidelines for Oasis v4 Development

Access and usage of the Oasis v4 web application is determined by the user having specific application roles assigned to them. When developing functionality, sufficient application roles should be used to control the access (read only), creation and modification of business objects. If a user does not have at least read only access, then the page or piece of functionality should not be accessible and will not be displayed in navigational areas.

The service desk/infrastructure team are responsible for managing Active Directory groups and will assign app roles to security groups on request via a Service Desk ticket.

If a user's security token is retracted in the Azure portal, the user should be signed out of Oasis v4 on the next internal token refresh.

Version of new production systems for Oasis v4 need to be authorized by the Development Manager or Operations Director before they can be deployed.

2.5 Secure customer data

All customer credit card details and passwords must be encrypted within the Oasis database. Only members of the Oasis_CreditController and Oasis_CreditControllerManager active directory groups can have access to any credit card information held in Oasis.

Customer passwords cannot be retrieved if forgotten or viewed by any user of Oasis. In the event of a forgotten password Oasis will reset the password and email the customer with the new login information.

We do not process customer payments on any web applications, payments are processed by the credit control team and an invoice is sent out.

2.6 Third Party associations

Any third-party or external development that has access to the information held within Oasis must adhere to the following:

- password protected, or windows authentication access to the system
- if web based, must only be accessible via HTTPS
- Never display user password information in any admin modules.

- Must be approved by the Operations Director and either the Development Manager or Business Process Manager.

2.7 Secure repositories

All source code is stored in Azure DevOps in a collection of Git repositories, which are restricted to members of the development team and certain key stakeholders. Access to source code is controlled by the Development Manager. The source code repository allows for:

- Granular permissions to be defined - https://msdn.microsoft.com/en-us/library/ms252587.aspx
- Version control of source code
- Feature branches and code review via pull requests
- Auditing and Reporting

2.8 Code reviews

Azure DevOps has a mechanism to enforce code reviews through feature branches and pull requests. Pull requests are a mechanism to allow other team members to review the changes, make comments where they believe further changes should be made (e.g. incorrect functionality, code maintainability, code style etc) and when satisfied, approve the request which allows the merge to take place. Code can only be merged into the main development branch through a pull request and each pull request requires at least one approver. The creator of the pull request can't approve their own request. All new projects require a pull request approval, and this is being implemented in older legacy projects.

2.9 Static Code Analysis

Static code analysis at compile time is performed by Microsoft Roslyn analysers which are added to the project being built. The analysers check the project for various design, naming, performance, maintainability, reliability, and security issues.

2.10 Automated Testing

Automated Testing is done using Ranorex Studio to ensure the critical path through the application remains stable and unchanged. We have a standard dataset requirement for the automated testing to ensure consistency in each development build.

Version Control

Author	Version	Date	Description
Clare Metcalfe	1.0	14/09/2015	Original
Clare Metcalfe	2.0	15/03/2016	Code Review Addition
Clare Metcalfe	3.0	25/09/2018	OWASP version/CC Validation update
Clare Metcalfe	4.0	01/04/2020	Annual review – no changes
ISC	4.0	02/04/2021	Annual review - no changes
Kev Wootton	5.0	02/09/2021	Updated for new procedures
Jason Parsons	6.0	31/08/2022	OasisV4 additions
Jason Parsons	6.0	06/09/2023	Annual review – no changes

Document Approval

Name	Version	Date	Position
ISC	1.0	14/09/2015	Information Security Committee
ISC	2.0	15/03/2016	Information Security Committee
ISC	3.0	25/09/2018	Information Security Committee
ISC	4.0	01/04/2020	Information Security Committee
ISC	4.0	02/04/2021	Information Security Committee
ISC	5.0	02/09/2021	Information Security Committee
Clare Metcalfe	6.0	30/09/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 30/09/2022