

Secure Development Policy

Policy Owner: Dan Pupek

Effective Date: 07/15/2022

Purpose

To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Scope

This policy applies to all employees of Darwin Global or its divisions and its wholly-owned subsidiary and to all external parties with access to Darwin Global engineering data/information, information systems, networks, and system resources.

All Darwin Global LLC applications and information systems that are business critical and/or process, store, or transmit confidential data. This policy applies to all internal and external engineers and developers of Darwin Global LLC software and infrastructure.

Policy

This policy describes the rules for the acquisition and development of software and systems that shall be applied to developments within the Darwin Global LLC organization.

System Change Control Procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. Change control procedures and requirements are described in the Darwin Global LLC Operations Security Policy.

Significant code changes must be reviewed and approved by the Chief Software Architect or a Senior Engineer before being merged into any production branch in accordance with the release cycle found here:
https://docs.google.com/presentation/d/1Cze1YX5em7OmjvGgtTRCzYkM9hFJ_UurTf6l9e-Hnso/edit?usp=sharing

Software Version Control

All Darwin Global LLC software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role. All code is written, tested, and saved in a local repository before being synced to the origin repository.

Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, business-critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

Restrictions on Changes to Software Packages

Modifications to third-party business application packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Secure System Engineering Principles

Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts.

Engineering style guides and technical references can be found in the NexPort Development Wiki here: https://darwin-global.fogbugz.com/f/page?W4349

Software developers are expected to adhere to Darwin Global LLC's coding standards throughout the development cycle, including standards for quality, commenting, and security.

Secure Development Environment

Darwin Global LLC shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development

Outsourced development is generally discouraged within Darwin Global LLC. In the event outsourced development is required, Darwin Global LLC shall supervise and monitor the activity of outsourced system development. Outsourced development shall adhere to all Darwin Global LLC standards and policies.

System Security Testing

Testing of security functionality shall be carried out during development. No code shall be deployed to Darwin Global LLC production systems without documented, successful test results.

System Acceptance Testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new versions.

Prior to deploying code to production, a Test Plan MUST be completed which shows the completion of all associated tests.

Protection of Test Data

Test data shall be selected carefully, protected, and controlled. Confidential customer data shall be protected in accordance with all contracts and commitments. Customer data shall not be used for testing purposes without the explicit permission of the data owner and the Chief Software Architect.

Acquisition of Third-Party Systems and Software

The acquisition of third-party systems and software shall be done in accordance with the requirements of the Darwin Global LLC Third-Party Management Policy.

Exceptions

Requests for an exception to this Policy must be submitted to the Chief Software Architect for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Chief Software Architect or any other members of management or operations. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	07/15/2022	SOC2/2022	Diana Hussein	