





Operation/Task:	SDLC Process for Development			Equipment:	N/A
Owner:	Vice President of Technology	Date Created:	5/27/20	Department:	IT
		Revision History:	See last page		

ALERTS (see below): Critical Step  Quality Check  Tip  Team Safety 

Purpose: This SOP/work instruction documents procedures for secure application development and testing.

Step #	Alerts	Step Description - "What to Do"	"How to Do it"	"Why to Do it"
1		Project Initiation The following Risk Analysis is documented in the Discovery Guide, plus in either the subsequent Statement of Work (SOW) or else documented in the Project Change Request (CR) document.	<ul style="list-style-type: none"> - Conduct Initial Risk Analysis <ul style="list-style-type: none"> o Information Classification <ul style="list-style-type: none"> ▪ Profile Information ▪ Uploaded data ▪ User Entered o Legal/Regulatory/Reputational Risk (Customer Driven) o Public/Customer Facing 	
2		Functional Design Analysis and Planning The following are documented in the Statement of Work or Change Request documents.	<ul style="list-style-type: none"> - Website Requirements - Website Features - Implementation Plan (high level) - 3rd party Static Analysis Software - Testing be conducted for all custom code - Type of test systems needed (usually just Pageflex) - Develop business/user test plan (in Implementation Plan) - Should peer code reviews be conducted (see Discovery Guide) 	
3		System Design Specifications The following are in the Statement of Work or Change Request documents	<ul style="list-style-type: none"> - Customer Requirements or Features - Technical Developer Designing/Planning 	
4		Software Development Development requirements are outlined in the "OWASP Top 10" document (or subsequent documentation). Coding Standards are documented in the ENPOINTE IT SOPs.	<ul style="list-style-type: none"> - Validate requirements are being met in the SOW or CR. 	

5		Implementation	<ul style="list-style-type: none"> - All testing is to be done in a testing environment. - All .DLLs and .Exe's are to be scanned by a 3rd party static vulnerability system. The scan results should not contain any High or Critical security bugs. - All production deployments need to be submitted through Track-It. The Track-It must include a Deployment Guide and the results document from the Static Analysis Software Testing scan. - Documentation will be reviewed by the development manager prior to production deployment. 	
6		Operational/Maintenance	<ul style="list-style-type: none"> - Indicated how this will be maintained going forward <ul style="list-style-type: none"> o Support, patching... (Included in SOW) 	
7		Disposal	Data disposal standards will follow the standards are documented in the ENPOINTE IT SOPs.	

Notes:

Definitions:

Revision History	Description of Changes	Requested by	Date
Rev 1	First posting to intranet	Dave Johnson	5/27/20
Rev 2	Changed GLS References to ENPOINTE	Cristi Oakvik	3/10/21
Rev 3	Changed owner to Director of Business and Custom Applications	Mike Starrett	5/26/23
Rev 4	Updated document owner to Vice President of Technology	Mike Starrett	11/4/24