**Application Security Checklist**

<Project Name>

**Date:**

**Version No:**

**Document Instructions:**

* *Text in blue colour is to guide you in filling the document, you need to delete this blue text once document has been completed*
* *File name should be renamed as per the following naming standard:*

*SBU – Name of Project – Type of Document – version number e.g.:*

*Academy – Website Development – Vision and Scope – v0.1*

* *The page footer dynamically shows the file name, once you rename the file as per the above naming standard, you need to update the footer as well. To do so, simply open the footer (by double clicking on it), right click on the file name field within the footer and select Update Field. DO NOT MANUALLY TYPE THE FILE NAME*
* *Ensure you have the same document version number on the front page, footer and on page 2*
* *You need to replace the text within the brackets < > with the relevant information. Please remove the brackets once text is updated e.g.: On page 2,* ***Document Approval Table****, the text* **<SBU>** *should become* **Academy**

****

**Document Information**

|  |  |
| --- | --- |
| Criteria | Details |
| Document title: |  |
| Program Name: | *Enter the program ID & Name allocated for this project as per this format: <Program ID.Program Name>* |
| Vision & Scope Name: | *Enter the VnS ID & Name allocated for this project as per this format: <VnS ID.VnS Name>* |
| Project Name: | *Enter the project ID & Name allocated for this project as per this format: <Project ID.Project Name>* |
| Complete Project ID: | *Enter the complete project ID allocated for this project as per this format: <Program ID.Vns ID.Project ID>* |
| Document owner: |  |
| Document author: |  |
| Version: |  |
| Issue date: |  |

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Updated by: |
| 0.1 |  |  |  |
| 0.2 |  |  |  |
| 1.0 |  |  |  |

**Document Approval**

This document requires the following approval:

*Refer to the ADP Document Roles & responsibilities matrix and update the table below accordingly*

| Name/Position | Action | Signature | Date |
| --- | --- | --- | --- |
| **<SBU>** | | | |
|  |  |  |  |
|  |  |  |  |
| **<President’s Office>** | | | |
|  |  |  |  |

**Glossary & Acronyms**

| Name/Position | Description |
| --- | --- |
| AZF | Aspire Zone Foundation |
| AL | Aspire Logistics |
| SoD | Segregation of Duty |

**Contents**

[1. Introduction 5](#_Toc444594104)

[1.1 Purpose 5](#_Toc444594105)

[2. Checklist 6](#_Toc444594106)

[2.1 Logging 6](#_Toc444594108)

[2.2 Web Application Scanning 6](#_Toc444594109)

[2.3 Web Application Firewall 7](#_Toc444594110)

[2.4 Authentication, Access and Authorization 7](#_Toc444594111)

[2.5 System Acquisition and development Compliance 8](#_Toc444594112)

[3. Appendix 9](#_Toc444594113)

1. Introduction

## Purpose

This checklist is intended to ensure that minimum Application security activities are performed during the development of this project. This checklist shall act as a general guide for the proper development of the production environment and control improvements.

1. Checklist

## Logging

| No. | Description | Yes/No/N.A | Remark |
| --- | --- | --- | --- |
| 3.1.1 | Application is configured to send the alerts to the management Servers and to appropriate users |  |  |
| 3.1.2 | Application is configured to send the logs to the logging servers |  |  |

## Web Application Scanning

| No. | | Description | Yes/No/N.A | Remark |
| --- | --- | --- | --- | --- |
| 3.2.1 | Application has undergone Vulnerability assessment and all the critical and Medium vulnerabilities are mitigated |  |  | |
| 3.2.2 | Developed web application has undergone the following security tests before deploying in production (but not limited to): |  |  | |
| SQL injection |  |  | |
| Cross Site Scripting (XSS) |  |  | |
| Cross Site tracking (XST) |  |  | |
| Web Page code analysis |  |  | |
| Parameter Manipulation |  |  | |
| Form Field Manipulation |  |  | |
| URL Manipulation |  |  | |
| Session ID Security |  |  | |
| Access Control |  |  | |
| Directory traversal |  |  | |

## Web Application Firewall

| No. | Description | Yes/No/N.A | Remark |
| --- | --- | --- | --- |
| 3.3.1 | Application has undergone the WAF transition from transparent mode to the blocking mode and all the critical and Medium attacks detected are fixed in the application or blocked in the WAF. |  |  |

## Authentication, Access and Authorization

| No. | Description | Yes/No/N.A | Remark |
| --- | --- | --- | --- |
| 3.4.1 | All default passwords have been changed |  |  |
| 3.4.2 | Access Control has been configured on the application to allow authorized personnel only |  |  |
| 3.4.3 | Authorized personnel is authorized to perform intended task on need to know bases only |  |  |
| 3.4.4 | Developed application/software has been tested for the following security features before deploying in production (but not limited to): |  |  |
| Authentication |  |  |
| Authorization |  |  |
| Confidentiality of data |  |  |
| Integrity check |  |  |
| Input validation checks |  |  |
| Processing security controls |  |  |
| Output security controls. |  |  |
| 3.4.5 | SoD is in place for the data to be processed / generated in the Application. |  |  |
| 3.4.6 | Access to Information Systems storing the source codes shall be restricted to authorized users as per Access Control Policy. |  |  |
| 3.4.7 | Access to application/software shall be granted according to SoD matrix to avoid conflict of interest. |  |  |
| 3.4.8 | Quality Assurance team has performed the test of the codes developed by the development team as per Segregation of Duties (SoD) Policy. |  |  |

## System Acquisition and development Compliance

| No. | Description | Yes/No/N.A | Remark |
| --- | --- | --- | --- |
| 3.5.1 | Data input to application/software has been validated to ensure that it is correct and appropriate |  |  |
| 3.5.2 | Rules for checking the valid syntax of application/software inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content |  |  |
| 3.5.3 | Internal validation checks are incorporated into application/software to detect any corruption of the data processed |  |  |
| 3.5.4 | Restricted test data in QA environment shall be scrambled or masked |  |  |
| 3.5.5 | Appropriate compensating controls are considered, if any of the information security requirements are not met by the proposed information system, along with the risks due to lack of such information security control and its impact on business |  |  |

1. Appendix