Status: *Live*
Version: *1.1*

DIAGEO

Secure Development Lifecycle (SDL) Policy




This document contains proprietary information. ALL INFORMATION CONTAINED HEREIN SHALL BE KEPT IN CONFIDENCE. None of this information shall be divulged to persons other than Diageo and its trusted partner employees authorised by the nature of their duties to receive such information, or individuals or organisations authorised by Diageo in accordance with existing policy regarding release of company information

Table of Contents

Policy Statements

All software projects will follow this policy document.

1.1 Building Security In

For Diageo to have secure software systems, security must be included in the development process. Enumerated below are the methods in which this SDL process will be embedded into Diageo's PMO and SDLC methodologies:

- Security by Design: IM&S will provide application security (AppSec) guidance and best practices for software development projects, including:
    - Minimize the Attack Surface.
    - Establish & Use Secure Defaults.
    - Establish & Use Defense-in-Depth.
    - Use Nonstandard Configurations for Obfuscation.
    - Follow Industry Supported Secure Coding Guidelines and Best Practices.
    - Validate:
        - Error / Exception Handling.
        - Secure Software Supply Chain.
        - Session Management.
        - Memory Management.
        - Encoding.
        - Authentication.
        - Authorization.
        - Accountability.
        - Cryptography.
        - Privacy.
        - Data Validation / Sanitation.
- Testing: IM&S will leverage security testing, when appropriate for software development projects.

1.2 AppSec Architecture (ASA)

IM&S will provide input on high and medium risk projects, including advisory tasks regarding ASA solutions, such as: application-based edge protections (e.g., WAF, CDN, ELB), and / or vetted AppSec libraries (e.g., ESAPI).

Deliverables

- IM&S advice on security requirements to the relevant project manager. Where relevant, report of security testing of the software asset

Glossary, Acronyms and References

Term	Definition
PMO	Project Management Office – PMOs provide program and project governance to enterprises.
WAF	Web Application Firewall – A device used to filter insecure HTTP traffic.
ELB	Elastic Load Balancer – A device used to enable high availability via request workflow optimization.
CDN	Content Delivery Network – A device used to cache static content across geographic regions to ensure a high quality-of-service (QoS).
SDLC	Software Development Lifecycle – A methodology used for developing software.
ESAPI	Enterprise Security API – An AppSec-focused API for multiple languages developed by OWASP.

Audience

Technical staff (e.g. Global Operations & Engineering, Enterprise Architecture, TCS and other vendors) should review and adhere to this document when developing and / or maintaining software systems for Diageo. Any areas a vendor cannot comply with should be referred to IM&S for advice.

Scope

The scope of this document includes a documented, repeatable approach for developing secure software systems while it is also a complementary guidance for Diageo's project management office (PMO).
All processes and procedures referred to in this document are defined as Global in nature and therefore must be adhered to globally.

Objectives

The objective of this document is to ensure that software systems are developed in a secure manner for Diageo. This should be achieved regardless of the source of development or the platform on which the software is developed for (e.g., mobile, cloud, Web, ERP, desktop).

Exceptions

Exceptions to this Policy can only be granted in accordance with the Diageo IM&S Policy Framework. Applications for exceptions are requested through the ServiceNow and via the Diageo Information Security Exception Approval Process.

Incident Reporting

Any failure to comply with this document or security incident that materializes relating to the requirements within this policy must be reported to the Diageo Computer Security Incident (CSI) team by email at CSI@Diageo.com immediately.

Document History

Document Location

The current document will be held online in the Diageo Mosaic repository:

Site: Mosaic IM&S Document Library

Directory/File: Policies Folder

This file will also be available for Diageo Employees in the IM&S Codes & Policies public site on Mosaic.

Printed copies are valid only on the day of printing. It is the responsibility of users of this document to ensure they are using the most recent version. If the online location is not reachable, a copy of this document can be obtained from the Global IM&S team.

Revision History

This document is subject to Change Control and as such any amendments must be carried out through the Document Change Management process and all Approvers must agree the amendments.

Date of this revision	30th June 2017	Date of next review	14th Apr 2018

Version Number	Revision Date	Change History	Changes Marked	Updated By
1.1	30 June 2017	Reporting requirements and irrelevant terms from the 'Glossary' have been removed to achieve simplicity, no significant changes were made to the content		Tamas Sziller
1.0	12 June 2016	Document created	No	Steven Markey

Reviewers

This document requires to be reviewed by the following reviewers.

Name	Title	Review Date
John Haren	IM&S Head of Governance, Risk & Compliance	30 June 2017
John Merritt	Global Information Security Director	Feb 2017
Craig B. Fisher	Application Security Lead	May 2016
Stuart D. Holmes	Global Security Engineering and Ops Lead	Feb 2017

Approvals – Document Signoff (acceptance)

This document requires following approvals.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	30th June 2017

Distribution List

Once complete, this document will be distributed to:

Title (including company)
Above Approver List
Enterprise Architecture Team
Global Development Team
Tata Consulting Services
Governance, Risk & Compliance

The Accountable Party for this Policy coordinates and insures that the document is completed. This individual as well as others in the IT areas may also contribute in a collaborative fashion as is often necessary.

End of Document