Status: *Live*

Version *1.3*

DIAGEO

Third Party Information Security Governance Policy




Table of Contents

Policy

This document specifies the documents (i.e., policies, standards) that a third party should review and approve before being on-boarded by Diageo. This applies to any third party regarding the procurement of computer devices, networks, applications, and / or services that are creating, processing, transmitting, and / or storing Diageo information Assets (see glossary for further details)

We must ensure that whenever Diageo Information Assets are hosted on third party services, that they receive an equivalent level of protection to data hosted internal to Diageo. Failure to ensure this, means that such Information Assets might be unnecessarily exposed to the public or other organisations, resulting in damage to Diageo's reputation, brands, loss of personal data, distress to individuals and loss of revenues

1.1 Policies & Standards for All Deployments

Whenever you contract with third parties, who host Diago Information Assets, those parties must be bound by a contractual obligation to comply with the following policies and standards (where relevant to the service being provided).:

- Information Handling Standard
- Acceptable Use Policy
- Data Destruction Standard
- Information Retention Standard
- Authentication Standard
- Privileged Access Management Standard
- Access Management Standard
- Cryptography Standard and Database Cryptography Standard
- Threat & Vulnerability Management (TVM) Standard
- Logging Standard
- System & Network Security Standard
- Third Party Hosting Standard
- Network Firewall Policy
- Physical Protection Standards
- Industrial Security Control Standard

1.2 Policies & Standards for Custom / Modified Development

Whenever Diageo contracts with a third party to procure and/or update a custom or modified system / application software, that third party must be subject to a contractual obligation to comply with the following policies and standards: :

- Secure Development Lifecycle (SDL) Policy
- Secure Coding Standard

1.3 Right to Audit

Diageo must have the right to verify the vendor's degree of compliance with Diageo policies, standards, and procedures. An alternative to this may be the delivery of an independent audit report from the vendor (at Diageo's request) to provide the relevant security assurance.

1.4 Due Diligence

Diageo will ensure that proper due diligence is performed while selecting or on-boarding a vendor, to include:

- security assurance (self-assessment) review
- the completion of the Managed Services Checklist (for software-as-a-service [SaaS], hosting, or co-location providers)
- a request for Diageo Legal to engage in a privacy impact assessment (PIA) where services involve processing of Highly Confidential Information, PII and/or Special PII

1.5 Confidentiality and Data Protection

In addition to physical security requirements, all Information Assets hosted on Third Party Systems must be made subject to a contractual obligation to maintain the confidentiality of all Diageo data held and/or processed by that party.
With regards to PII and Special PII, all third parties processing such data, must be made subject to lawful data processing outsourcing clauses, as set out in our 'IM&S template for contract additions' document. Any contracts which involve the processing of PII and/or Special PII should be referred to the legal department for sign off, prior to entering into the agreement with the provider.

1.6 Glossary, Acronyms

Term	Definition
Personally Identifiable Information (PII) ***Data that directly or indirectly identifies an underlying individual***	Information relating to an identified or identifiable natural person ('data subject'); including by reference to an indirect identifier such as a code, identification number, Internet Protocol address or geolocation data, a cookie, pixel or other online identifier. *Always check with the legal team whether any form of PII needs to be encrypted pursuant to local regulations (e.g. Social Security Numbers in certain US States) or if a Privacy Impact Assessment needs to be conducted and encryption is recommended e.g. for bulk processing of PII or PII which relates to high risk processing activities,* **prior** to the commencement of such processing.

Term	Definition
Special PII	***Special PII****:* ▪ *Information about a person's* racial or ethnic origin ▪ *His or her* political opinions ▪ *His or her* religious or philosophical beliefs ▪ trade union membership (except in the US) ▪ His or her genetic data ▪ His or her biometric data to uniquely identify a natural person ▪ data concerning health or data concerning a natural person's sex life or sexual orientation *Information which, if compromised, could result in harm to the individual and therefore should be minimised for the purpose and treated as Highly Confidential and encrypted in transit and when data is stored.* As noted above, you should consult the legal team whenever processing Sensitive PII to assess what security controls and/or Privacy Impact Assessments may need to be carried out in relation to such activities **prior** to the commencement of such processing.

Audience

All Diageo employees, employees of subsidiaries and joint ventures, consultants, contractors, and third parties with access to Diageo information or information systems or who maintain information on Diageo's behalf are responsible for complying with this Policy.

Scope

The scope of this policy is applicable to all applications, systems, devices, and peripherals resources owned, leased, and operated by Diageo where such Information Assets and applications are hosted externally using systems and premises not owned by Diageo

Objectives

This Third Party Governance Policy is established to achieve appropriate and acceptable vendor governance practices in accordance with applicable law and other rules and regulations in order to ensure Diageo data maintained, stored and managed on third party services is properly secured and treated with the correct minimum levels of care

References

Soft copies of the referred Policies and Standards can be located within the IM&S Policies, Standards & Guidelines Public site located on Mosaic.

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 via the Diageo Information Security Exception Approval Process.

Incident Reporting

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

Document History

Document Location

Soft copies of this documentation can be located within the IM&S Policies, Standards & Guidelines Public site located 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 Information Management and Security 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	30 June 2017	Date of next review	20 Apr 2018

Version Number	Revision Date	Change History	Changes Marked	Updated By
1.3	27 June 2017	Updated with sections about 'Confidentiality and Data Protection, 'Glossary and Acronyms' and minor updates were also made to wording.	No	Tamas Sziller
1.2	15th Sept 2016	Lists have been updated in sections 1.1 and 1.2	No	Tamas Sziller
1.1	6th Sept 2016	Document updated based on inputs from David Johnston	No	Tamas Sziller
1.0	13th June 2016	Document created Former Third Party Hosting Standard was also merged to this Policy	No	Steven Markey

Reviewers

This document requires to be reviewed by the following reviewers.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	June 2017
John Merritt	Global Information Security Director	June 2017
Craig B. Fisher	Application Security Lead	June 2017
Stuart D. Holmes	Global Security Engineering and Ops Lead	June 2017
Brendan Fedigan	Solution Architect NAM, IS Service	June 2017

Approvals – Document Signoff (acceptance)

This document requires following approvals

Name	Title	Review Date
John Haren	IM&S Head of Governance, Risk & Compliance	27 June 2017

Distribution List

Once complete, this document will be distributed to:

Title (including company)
Above Reviewer/Approver List
IM&S Yammer Community

End of Document