Status: *Live*

Version *2.0*

DIAGEO

Third Party Hosting Standard




1. Contents

1. Standard

This document defines the requirements that third parties must comply with when hosting a web application or web service for Diageo, where the systems hosting the site are not located on Diageo property.

1.1 Data Classification

As a matter of policy Diageo seeks to protect its data on the basis of the sensitivity of that data. Diageo does this by assigning a classification to data. This allows for more extensive protection of particularly sensitive data and more cost-effective security for less sensitive data. In order of increasing sensitivity the classifications used by Diageo are:

- **General**: Information that can be disclosed without risk of damage or harm to the interests of the Diageo (e.g. public press releases approved by corporate relations, media reports. . It may be inappropriate to share General Information Assets externally, or with everyone internally, e.g. global newsletters, Mosaic content, routine emails *etc.*

- **Confidential**: Information that, if subject to unauthorised disclosure (even within Diageo), could cause damage or harm to the interests of Diageo, its subsidiaries and joint ventures in which Diageo has a controlling interest, e.g. business plans, Personally Identifiable Information, financial and marketing information, etc. Only authorised employees should have access to such Information Asset(s).

- **Highly Confidential**: Information that, if subject to unauthorised disclosure (even within Diageo):
    - Could cause material damage or significant harm to the interests of Diageo, its subsidiaries and joint ventures in which Diageo has a controlling interest; or
    - That is prohibited by law or regulation from being disclosed, e.g. share price sensitive information, such as merger and acquisition activity; proprietary information, such as product recipes; and Special Personally Identifiable Information Assets. Only those for whom it is necessary to do their job should have access to such Information Assets.

A confidentiality agreement/ NDA or other duty of confidentiality should be in effect with Third Parties.

If materials are not classified, you should classify the document in line with the Classifications set out in Information Handling Standard *and/or consult with the Diageo legal team.*

More detailed explanations of these classifications are available in the Information Handling Standard. Diageo persons looking to host with a third party are responsible for determining the correct classification of that data.

1.2 Requirements Applicable to All Hosting

1.2.1 System Configuration

Systems must be hardened in accordance with relevant best practice. At a minimum this must include:

- **Disabling of services**: All non-essential network services that must be disabled. Preference must be given to the use of services that are encrypted.
- **Software installation**: Only required software and operating system components are to be installed. Any unnecessary software or operating system components must be removed.

- **Patching**: A schedule must be in place and adhered to for the regular installation of all patches released by the manufacturer of any software in use.
- **Logging**: At a minimum logging must be retained for 90 days. Any activity relating to authorisation, approvals or use of privilege must be logged. Where legal or regulatory requirements are in effect it may be necessary to hold logging data for longer, where such requirements are in existence compliance is required.
- **Anti-Virus**: All operating systems for which suitable anti-virus is available must have this installed. Anti-virus must be configured to automatically update in accordance with the manufacturers guidelines.
- **Remote system access**: Any network access to the underlying system be must over an encrypted connection.
- **Privileged access**: Any privileged access must be on a least privilege basis only. Privileged access must be reviewed every month, three months or six months depending on tiering of the system/application to ensure a Continuous Business Need (CBN).

1.2.2 Network Architecture

- **Firewalls**: Connections from the Internet, management networks or other network segments must be controlled via the use of firewalls. Firewalls must be configured with a default deny policy and grant explicit access only for those systems and services for which it is required. Rules allowing access from any location or using any service are not permitted.
- **Segmentation**: For Internet facing applications, the database server should always be in a trusted data centre location, not in the DMZ. Application servers and database servers must be in a separate logical zone from any networks that are used for testing or development. Diageo processing should be logically separated from the 3rd party's other customer and tenant data if possible.
- **Intrusion Detection**: An appropriate intrusion detection/protection solution must be deployed to protect any connection exposed to the Internet. Sensors must be appropriately tuned to minimise false positives while still detecting inappropriate activity. IPS logs must be reviewed at least daily for alerts.
- **Logging**: All firewall and IPS traffic must be logged for 90 days minimum, more where there is a legal or regulatory requirement to do so.

1.2.3 Encryption

Where encryption is deployed as part of a solution the following requirements must be met:

- **Algorithms**: Only non-proprietary algorithms, which have been subject to public scrutiny, are to be used.
- **Key Length**: The length of encryption keys must be chosen such that they cannot be easily guessed using a brute force attack.
- **Encryption Keys**: Keys must be protected and handled in a manor appropriate to the sensitivity of the data they protect. At a minimum they must be treated as Confidential.
- **Key management**: A key management process needs to be in-place and it should be ensured that keys are protected at all times. Keys should be destroyed in a manner that does not expose the protected data.

1.2.4 Application Design

Minimum application design requirements are as follows:

- Only functionality or application modules that are required as part of the solution are to be used.
- Applications or libraries must be installed in accordance with the manufacturer's recommendations.
- Bespoke applications must be developed in accordance with Diageo's secure coding standards – these will be supplied separately if required.
- An appropriate process must be used to ensure that code can only be progressed from production/test environments to the live environment by authorised individuals and after it has been adequately security tested.
- Best practice coding must be implemented, e.g., in accordance with OWASP top 10 or similar Secure Development Life Cycle (SecDLC).

1.2.5 System Backup

Systems must be backed up. At a minimum the following regime must be followed:

- A daily backup must be made and retained for 30 days. Incremental backups are permissible however a full backup must be made at least weekly.
- A monthly backup must be made and retained for 12 months
- Personally Identifiable Information (PII) or Highly Confidential Information or Confidential Information backups are encrypted

Regulatory requirements may mandate that a different or extended backup regime be used.

1.2.6 Disaster Recovery

Provisions must be in place to ensure continuity of service, and Service Level Agreements (SLAs) are met in the event an incident or disaster renders the primary hosting location unavailable for an extended period of time.

1.2.7 Secure Disposal

Systems hosting of Diageo data must be securely erased before disposal and any related documentation must be destroyed to an unrecoverable state after use. At a minimum, magnetic media must be positively overwritten using disk wiping software. As mandated in the Diageo Data Destruction Standard (Please request a copy if needed).

1.2.8 Compliance

A confirmation by the vendor of compliance to "Third Party Hosting Standard' is required when the contract is signed and also in the case when there is a change in the service.

1.2.9 Independent Security Attestations

System and Organization Controls (SOC) reports, Payment Card Industry (PCI) attestations of compliance, and International Organization for Standardization or ISO 27xxx certification are valued by Diageo. Diageo encourages service providers to obtain and submit copies during procurement negotiations of, e.g., ISO27001/2 are preferred for foundation Security controls, ISO 27017 for Cloud Service and ISO 27018 for GDPR or personal data protective controls attestations. A latest penetration test report conducted by an independent auditor should be provided.

1.2.10 Personally Identifiable Information (PII) and Financial Information

If PII and financial information are to be held or processed then the system must be treated as handling Confidential Data at a minimum with appropriate encryption on storage, processing and transmission activities.

1.2.11 Training

All vendors must confirm to Diageo that their staff have been trained in the requirements of data protection law, security, PCI (if handling credit card data) and are subject though their employment contracts to a duty of confidentiality. All vendors must be approved by Diageo legal prior to any data transfer taking place.

It is mandatory that service providers and their staff handling Diageo PII are trained to:

- Apply a security incident management process, technical staff training and customer notification to handle data breaches informing csi@diageo.com.
- Understand the consequences of data privacy breaches of personally Identifiable Information (PII) data.

1.2.12 Physical Security Requirements

If PII and financial information are to be held or processed then the system must be treated as handling Confidential Information.

- If the data centre or hosting facility occupies an entire building then physical security consideration must be given to the exterior of the building, lobby areas, utility areas, loading bays, offices and sub-areas of strategic rooms or floors that hold IT equipment.
- If the data centre occupies part of a building, then physical security consideration must consider relevant office space and strategic sub areas of rooms or floors.
- Access control and access management must indicate who has access, how access is granted, how visitors and vendors are managed and how to deal with breaches of access policies.
- Access reports must be regularly reviewed by someone with designated security responsibility, investigating and remediating process failures appropriately
- Procedures must be in place for securing selected equipment, cabling systems, encryption equipment, media rooms and storage cabinets or areas that contain sensitive data.
- Procedures must be in place for securing utility systems, including air conditioning, power supplies, network connections and emergency power systems against unauthorised access.
- Security procedures for business-hour operations, after-hour operations and emergency operations must be documented
- Inventory logs of Diageo managed equipment including serial numbers and configuration must be maintained
- Personnel with authorised access to confidential data must be documented and maintained.
- Procedures for managing environmental settings in data processing rooms must be documented
- Incoming and outgoing package control procedures must be in place.
- Suitable and sufficient fire suppression systems must be in place
- Sensitive material must be stored in suitable containers that meet minimum fire and burglary resistance standards
- CCTV must be used. At a minimum this must cover all entrances and exits for the data centre. Procedures must be in place for its use and maintenance.

1.2.13 Confidentiality and Data Protection

All Diageo Information Assets housed on third party systems must be subject to a contractual obligation to maintain the confidentiality of all Diageo data held and/or processed by the 3rd party according to the IM&S template for contract additions (Appendix 'A').

With regards to PII and Special PII, all third parties processing such data, are subject to lawful data processing outsourcing clauses,. Any contracts which involve the processing of PII and/or Special PII should be referred to the legal department to conduct a Privacy Impact Assessment (PIA) and sign off prior to entering into the agreement with the provider.

1.2.14 Data Retention

Diageo data must be retained for the duration of the retention period specified by Diageo, and disposed of securely once this retention period has been satisfied. Any relevant retention requirements will be supplied by Diageo. An attestation will be required from the vendor stating that all Diageo data has been securely disposed.

Agreements for the return of Diageo data at the end of the contract shall be agreed and built into contractual obligations with the 3rd party.

Diageo may temporarily suspend a retention period and require data to be preserved, for example during a regulatory investigation, litigation, tax audit etc. In such an event, the data must be protected from either manual or automatic deletion or alteration.

1.2.15 Website Deactivation

Websites must be deactivated when no longer in use. The further treatment of the Diageo data that was used by the website (including raw data, personal data, intellectual property, etc) is at the discretion of the application owner, but must be aligned to current Diageo IM&S Policies and Standards (e.g. Data Destruction Standard in case of disposal, etc)

1.2.16 email Hosting

Mail Exchange records must only be pointed to one of two places:

- Diageo's instance of Office365
- At an approved agency that has been appropriately evaluated. 'Evaluation' refers to the review and approval by Information Management & Security (IM&S), Procurement & Legal functions. The criteria for the approval include considerations such as appropriate retention, data privacy, security etc. It is essential that these are built into the contract with the agency. A Project Manager is accountable to ensure that agency has been appropriately approved by IM&S, Procurement & Legal before the MX record is pointed at that agency.

All other locations may point to a Mail Exchange record if the only functionality is to forward email to an approved email host. There should not be a valid mailbox on an unapproved email host.

1.3 Requirements for the Hosting of Confidential / Highly Confidential Information

Where Confidential Information will be hosted these requirements apply in addition to those requirements outlined in section 1.2

1.3.1 System Configuration

- **Authentication**: All access to Confidential/Highly Confidential Information must be authenticated and traceable to a unique user identity. All access across the Internet to Confidential Information or above must be strongly authenticated – this can occur at the application, system or network level.
- **Encryption**: All Confidential/Highly Confidential Information must be encrypted both at rest and in transit according to Cryptography Standard.
- **Logging**: At a minimum logging must be retained for 90 days Any activity relating to authorisation, use of privilege or approvals must be logged. Where legal or regulatory requirements are in effect it may be necessary to hold logging data for longer. Where such requirements are in existence compliance is required.
- **Host Intrusion Detection**: Systems hosting **Highly Confidential** Information must have an appropriately configured Host Intrusion Detection System installed.
- **Shared systems**: The use of shared systems is prohibited for the hosting of **Highly Confidential Information.**

1.3.2 Network Architecture

- **Segmentation**: Any system holding Confidential/Highly Confidential Information must be hosted in a network layer that is not directly accessible from the Internet.
- **Intrusion Detection**: Any traffic to a system hosting Confidential/Highly Confidential Information must be subject to either IPS or IDS. Logs must be monitored continuously or generate alerts out of hours, which will be acted on promptly.
- **Logging**: All firewall, IPS traffic, coperating system, web application, database, anti-virus and any other critical services must provide logging for 90 days minimum, more where there is a regulatory requirement to do so. The logging must include unsuccessful logon attempts, account/password creation, modification, or deletions. The logs should include sufficient information to reliably reconstruct the chain of events and track back to the authenticated user.
- **Remote access**: Single-Sign On (SSO) and Multi-factor Authentication tools are required for any kind of remote access (while travelling or at home). Mandatory for PII, PCI and other confidential data.
- **Administration**: Multi-factor authentication and unique accounts are required when doing technology or data administration.

1.3.3 Compliance

- **Right of Audit**: Diageo must have a right of audit to ensure that its Confidential/Highly Confidential data is being properly protected.
- **Compliance Monitoring**: Any system holding Highly Confidential Information must be subject to compliance monitoring.
- **Integrity Checking**: Any system holding Highly Confidential Information must be subject to automated integrity checking such that any unauthorised modification of files is automatically detected, investigated and prevented from recurrence

1.3.4 Hosting of Personally Identifiable Information (PII)

Personally Identifiable Information (PII and Special PII) relates to citizens data form a European or other country with specific data privacy or data protection laws such as the EU General Data Protection Regulation (GDPR). Adherence to where a Privacy Shield framework and agreement must be in place for 3rd parties locating data in the United States of America. It must also be approved by the Diageo Legal department, **prior** to any such transfer taking place. Preference should always be given to servers capable of hosting Diageo data within countries located with the European Economic Area for European citizens.

For a comprehensive guide to the requirements Diageo impose with regards to the handling and processing of PII and Special PII, please read the Diageo Data Protection Policy, which is incorporated into this Standard by reference and available upon request.

1.3.5 Processing of Credit Card Transactions

Any systems processing credit card data must be compliant with applicable portions of the Payment Card Industry Data Security Standard (PCI DSS) and other PCI-related application or service provider standards where applicable.

1.4 Additional Requirements for Third Party Hosting Utilizing Virtualization

1.4.1 Hardening

Virtualized hosts and operating system must operate with sufficient security controls with a hardened configuration to prevent outages and cyber-attacks.

1.4.2 Remote Access to Virtualized Host

Where the virtualization technology supports firewalling (of the hosted operating system), this must be enabled and adhere to best practice change management controls.

Single-Sign On (SSO) and Multi-factor Authentication tools are required for any kind of remote access (while travelling or at home) and when requiring elevated privileges to administer the technology or data. Mandatory for PII, PCI and other confidential data.

1.4.3 Logging

The virtualized host must be configured to send security sensitive log alerts to a central or remote host via syslog or similar method.

1.4.4 Host Management

Access to the host system must be through a dedicated management network interface which is not physically accessible from the virtual machines..

1.4.5 Maintenance of Virtual Machines

All Virtual Machines must be patched and have their antivirus adequately maintained. Unused virtual machines should be shut down. If this cannot happen, Diageo expects that regular patching and antivirus update schedules continue till they are shut down.

1.4.6 Protection of Virtual Machines from physical access

All virtual machines must be located on an encrypted partition such that physical compromise of the system will not grant access to the hosted systems. See 1.2.12 above for specific requirements.

1.4.7 Use of Virtualized Storage

Virtual storage systems must isolate Diageo data and meta data from other entities in a multi-tenant infrastructure model. If a shared approach to data separation is to be used then Diageo security must evaluate the design to ensure it is appropriately addresses any potential risks.

This document defines the requirements that third parties must comply with when hosting a web application or web service for Diageo, where the systems hosting the site are not located on Diageo property.

2. Definitions, Glossary, Acronyms

Term	Definition
Continuous Business Need (CBN)	The routine review of privileged access and user accounts to ensure that those accounts are still required.
Data	For the purposes of this document the term data is to be read as meaning either Sensitive PII, PII, Information Assets, data or information.
European Economic Area	The European Union (EU) Member States and the European Free Trade Association (**EFTA**) States (Iceland, Liechtenstein, and Norway).
External Hosting	External hosting is any hosting arrangement where services or applications are hosted on systems and premises not owned by Diageo.
Information Asset	Means: • Information, PII, Sensitive PII, data, meta-data, of all classifications in whatever form including images, still and moving, and sound recordings; and • those systems and processes which capture, store and deliver information as part of the service (e.g. databases, paper records, system information and documentation, hardware such as servers and networks, computer rooms, etc.).
Information Systems	All applications, systems, devices, and peripheral resources owned, leased and operated by Diageo or contracted with a third party by Diageo

Term	Definition
Least Privilege	The principle of granting privileges (or permissions) and access according to business needs.
Mandatory/Must	Used to denote that a specific item within this document is mandatory. An exception for such a requirement can only be granted with approval from the Diageo CISO or nominee.
Personally Identifiable Information (PII) **Data that directly or indirectly identifies an underlying individual**	Is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Always check with the legal team on whether any form of PII needs to be encrypted pursuant to local regulations or is 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, such as risk of an adverse risk on the individual* **prior** to the commencement of such processing.
Prohibited/Must Not	Used to denote that a specific item within this document is **not** permitted. An exception for such a prohibition can only be granted with approval from the Diageo CISO or nominee.
Special PII	Special PII is information which if compromised, could result in harm to the individual and therefore should be minimised for the purpose and, unless ad hoc low risk, treated as Highly Confidential and encrypted in transit and when data is stored. (*Such information includes, but is not limited to, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning medical/health or data concerning a natural person's sex life or sexual orientation)*.) 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.

3. Audience

Third parties and non-technical staff procuring technical services directly should provide this standard to the vendor and ask for confirmation of their compliance to the standard. Any areas the vendor cannot comply with should be referred to IM&S for advice.

Technical persons involved in the procurement of external hosted solutions are responsible for ensuring those solutions comply with the requirements of this standard

4. Scope

This standard applies to all hosting arrangements where applications are hosted externally using systems and premises not owned by Diageo.

5. Objective

There is increasingly a cost benefit in having various types of applications managed on offsite servers by third parties who specialise in the configuration and maintenance of those applications. In addition to cost benefits well run sites can offer various other benefits, such as better reliability, resilience and disaster recovery, than would often be available were an equivalent application hosted internally. This standard has been created in order to ensure Diageo data maintained, stored and managed on such services is properly secured and treated with the correct minimum levels of care. Diageo data hosted on third party services may not receive an equivalent level of protection to data hosted internal to Diageo. In turn this data might be unnecessarily exposed to the public or other organisations, resulting in damage to Diageo's brands, revenues and reputation

6. 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.

7. 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.

8. Document Information

8.1 Document Location

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

Server: IM&S Mosaic Site

Directory/File: IM&S Mosaic Standards

8.2 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	15/05/2018	Date of next review	15/05/2019

Version Number	Revision Date	Change History	Changes Marked	Updated By
2.0	15/05/2018	Requirements have been amended for: network segmentation; privileged access review; data protection, retention and disposal, website deactivation. New requirements added about: encryption key management; coding – OWASP; backup encryption; independent security attestations; training at vendor/service provider; authentication requirements for remote access and administration; PII data hosting.	N	Tamas Sziller
1.9	25/05/2017	Minor updates were added to the content to give more clarity and also references to the Database Cryptography and Cryptography Standards have been added in section 'Encryption'	N	Tamas Sziller
1.8	16/09/2016	Updated as part of PSG review process,	N	Tamas Sziller

8.3 Reviewers

This document requires to be reviewed by the following reviewers.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	15/05/2018
John Merritt	IM&S Director	22/05/2017
Jane Smith	IM&S Risk Specialist	14/05/2018
Ashirvad Roy	Information Security Manager	13/05/2018

8.4 Approvals – Document Signoff (acceptance)

This document requires following approvals.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	15/05/2018

8.5 Distribution List

Once complete, this document will be distributed to:

Title (including company)
BRM Community (to communicate to application owners)
IM&S Yammer Community

8.6 Related documentation

These documents can be found on the IM&S Document site on Mosaic.

1. Information Handling Standard.
2. Data Destruction Standard
3. System and Network Security Standard

The following document can be found on the Global policies site on Mosaic.

4. Data Privacy Global Policy

The Accountable Party for this Process 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 in IT Processes.

End of Document