Status: *Live*

Version *2.8.1*

DIAGEO

Systems and Network Security Standard




Table of Contents

Standards 3
1.1 Definitions 3
1.2 Classes of Diageo physical and virtual networks 3
1.3 Network Connectivity 4
1.4 Systems and Network Access 4
1.5 Network and Access Segregation 5
1.6 System Updates 6
1.7 Wireless LAN 6
1.8 Telecommunication Systems 7
1.9 Virtual Systems 7
1.10 Remote Access 7
Audience 8
Scope 8
Objectives 8
References 8
Exceptions 8
Incident Reporting 8
Document History 9
Revision History 9
Reviewers 10
Approvers 10
Distribution List 10

Standards

This standard defines the methods in which Diageo owned or managed systems and networks will be secured.

1.1 Definitions

Trusted Network: any class of network subject to all of the following:

- Lifecycle Management of connected devices, including (but not limited to) printers, scanners, IPT Handsets, servers, end user workstations
- Vulnerability Scanning of connected devices
- Regular Patching of connected devices for which there are known vulnerabilities and available patches.
- CBN (continual business need) review of access controls and/or firewall configuration. This process will be owned by Global Security Operations.
- Support for all connected network devices
- Managed Anti-virus software, regularly-updated, must be installed on all Windows-based devices
- Internet connections through Diageo's Secure Internet Gateways and/or proxy servers
- Segregated from untrusted or semi-trusted networks (see Section 1.3)

All other networks not subject to the above controls should be deemed untrusted. A semi-trusted network is one managed by a 3rd party, subject to their own controls, approved by IM&S.

1.2 Classes of Diageo physical and virtual networks

For the purposes of this document, the following "classes" of networks should be designated trusted (provided they are subject to the controls above), semi-trusted, and untrusted. Or as below:

Trusted

- Engineering Networks
- Main Corporate Production Networks
- Networks hosting SAP services and devices
- DMZ's
- PCI/POS Networks
- Voice networks
- Video Networks
- Corporate Wireless Networks
- Barcode scanning networks

Semi-trusted

- 3rd-party, cloud-based service provider or SAAS provider networks

Untrusted

- Guest Wireless Networks
- 3rd Party Interconnects
- Networks hosting legacy unpatched systems. Legacy systems are defined as systems or devices which can no longer be patched for security vulnerabilities, and for which known vulnerabilities exist.

1.3 Network Connectivity

- Diageo's internal network addressing scheme shall remain undisclosed and confidential, and internal addresses must never be publicized on the Internet. Beyond a dedicated site-to-site VPN connection, when accessing networks beyond Diageo's own network (i.e., the Internet), translation to a registered public Internet Protocol (IP) address must be done to mask Diageo's private IP address.
- Diageo users and systems, when connected to a Diageo network, must connect to the Internet via the internet proxy service.
- Web site address and content filtering exceptions, must be approved by GSO per the exception process.
- Network bridging to any Diageo trusted zone is not permitted, unless approved by IM&S
- The DMZ must facilitate proxy functions such as, authorization, audit, access control, and content inspection.
- Internet gateways must be designed, built, and configured (i.e., hardened) applying Diageo approved baseline standards, to be agreed and published by IM&S. These standards will be determined by Diageo, with input, if required, by IT outsourcers.
- ALL public Internet access mechanisms (e.g., SIGs, LIBO) must be approved by EA and GOE PRIOR to deployment to Diageo's infrastructure and production environments.
- All services, such as cloud, email, file transfer, and web browsing traffic will pass through approved Internet mechanisms and must be approved by IM&S, Global Operations, and Enterprise Architecture
- Business cases must accompany any request for Internet services.
- Mechanisms to circumvent SIG and/or proxy controls, unless approved by GSO, are prohibited.
- All Internet-facing hosts must be 'hardened' to appropriate standards, to include: all controls within Trusted Networks (see definition).
- Confidential and Highly Confidential files and Personal information transmitted or received from/to outside and within Diageo (email, uploads/downloads, transfers) must be encrypted in accordance with the Information Handling Standard and Cryptography Standard

1.4 Systems and Network Access

- Access and authentication to Diageo systems and / or networks must be in accordance with Diageo's Access Management Standard, Privileged Access Management Standard, and / or Authentication Standard.
- All servers, both physical and virtual, must be built using standard build scripts by the IT service provider (i.e., TCS and Verizon).

- For all windows-based, remote terminal logons, the screen must not display system or application identifiers until logon has been successfully completed. The display on the logon screen must include a general warning notice such as: "WARNING: This is a Diageo computer system. It is for authorised users only. It may only be used in accordance with Diageo's Computer Use Policies and may be subject to monitoring. Anyone found performing unauthorised activities may be subject to disciplinary action including criminal prosecution."
- Logon screens must not present help messages during the logon procedure (particularly warnings about how many incorrect entries are allowed.) Password reset instructions are excluded from this, as they are required to facilitate resets.

1.5 Network and Access Segregation

- Different classes of networks, as listed above, must be physically or logically separated. If the network is an engineering network, then, even if the network is trusted, it must still be separated (see below)
- IPS Systems, SPI (including layer 7 application inspection) and advanced threat detection must be deployed when connecting to/from:
    - The internet
    - DMZ networks
    - Networks hosting SAP services

- Dedicated security apparatus that may include firewalls or other relevant security threat management solutions, such as IPS, reverse proxies or application-level firewalls, must be used when connecting to/from: :
    - Engineering networks. Engineering networks (any network containing production and/or SCADA equipment) must be separated, even if their status is trusted.

  These solutions must properly mitigate any known vulnerabilities exposed by these connections. These vulnerabilities must be determined by a vulnerability scan . .

- IP-level, ACL-controlled separation between untrusted and trusted networks other than those detailed above, must be used, via switches, routers or VLAN configurations, or other layer 3 mechanisms.
- The Diageo corporate network must not be bridged or extended to other Diageo or third party networks without approval from IM&S, Enterprise Architecture, and Global Operations.
- All remote corporate network connections that originate from a non-Diageo managed network must traverse a gateway approved by Information Services (Enterprise Architecture, Global Operations & Engineering, and IM&S).
- Access controls between end-user devices and Diageo services must be implemented including:
    - Use of one-way trusts for authentication by systems hosted in legacy networks
    - VLAN access and configurations must be restricted to authorised users and systems only.
    - User access to systems and networks will align with Diageo's Privileged Access Management Standard and Access Management Standard.
- Defence-in-depth network protections mechanisms must be incorporated to include:
    - Firewalls will be deployed according to Diageo Firewall Policy.

    - IPS systems must be placed in active blocking mode after being optimized and tuned for ninety (90) calendar days.
- PCI Networks must be completely isolated from all other networks.
- Confidential or Highly Confidential data and personal information must be encrypted at rest. Transmissions of this data, for the purpose of transfer to other internal or external systems, must also be encrypted. Any transmissions featuring unencrypted credentials must be encrypted, regardless of confidentiality classification. Encryption techniques must be considered to be cryptographically secure.

1.6 System Updates

- Patch management of connected devices (including firmware updates) should be carried out in accordance with Threat and Vulnerability Management (TVM) Standard.
- An appropriate licence must cover all software programs and utilities used for Diageo business. Check licence terms with Legal Counsel before acceptance
- End-user Windows software which has not been centrally distributed, must be performed by TCS Desk Side Services. This is known as a Technical Install
- All such technical installs MUST be recorded for later audit
- End-users may not install their own desktop applications, unless they have been granted an exception to do so, via the Security Exception Process.

1.7 Wireless LAN

- Wireless access to Diageo's corporate network ("backbone", via wireless LANs [WLANs]) must be through a Diageo-managed wireless access point (WAP).
    - Guest WLANs must be logically or physically separated from the Diageo LAN in their route to the Internet.
- WLAN / WAP introductions require review and approval by GOE and EA
    - Enforcement will be satisfied by regular security testing.
- Diageo WAPs will be configured securely, via WLAN Controllers,, including:
    - Administrative interfaces will not be public facing.
    - Default configurations / credentials must be changed upon deployment.
    - SSID signal strength will not extend past 100 meters beyond a Diageo location.
    - Strong encryption (i.e., WPA2-Enterprise, TKIP / AES) for non-guest WLANs must be used, and will be in accordance with Diageo's Cryptography Standard.
        - The use of WEP is forbidden.
    - Logging on WAPs must be enabled.
    - WAPs must be physically secured by locating devices away from human access.
    - WAPs must not be installed in locations that make them susceptible to electromagnetic interference (EMI).
    - WAPs must fail-safe and revert to factory defaults when the device is reset.
    - WAPs and client firmware, operating system and utilities (drivers) must be updated in line with vendor recommendations.
- Wireless peer-to peer or ad hoc mode working is not permitted.

1.8 Telecommunication Systems

- Network Address Translation (NAT) must be implemented at VoIP segment to the public IP backbone.
- All VoIP traffic sent over a public IP network (e.g. Internet) must be encrypted in accordance with Cryptography Standard.
- VoIP systems and components must be deployed using a private address space.
- All VoIP perimeter firewalls must be securely configured to control protocols for call setup and termination. The perimeter firewalls must be dedicated to VoIP connections.
- Remote administration to voice servers and media gateways must take place through a secure remote access solution approved by IM&S.
- All critical servers, and services (e.g., SMTP, MS SQL, IIS), supporting the telephony environment must be hardened accordingly.
- Dedicated logical / virtual or physical server systems (e.g., a Windows Server for PBX services) should be explicitly deployed for telephony applications.
- All users must only be allowed to change voicemail settings via the phone interface or through an SSL connection. All HTTP and Telnet services must be disabled on the VoIP infrastructure
- All VoIP infrastructures must be kept current as per “trusted networks”.
- All VoIP voice servers and media gateways must be securely stored and managed within a physically restricted area accessible only by authorized staff.
- Any wireless telecommunications / VoIP functionality must comply with the WLAN requirements.

1.9 Virtual Systems

- Virtualization technology must support the logical separation of the guest operating system.
- Remote administrative access to a server / network from the internet must leverage VPN connections and two-factor authentication (2FA), and should leverage a jump (bastion) server, for access.
    - Drive mounting must be disabled.
    - Remote network access requires the use of a jump box / bastion host as well.
- Access to hypervisor management systems must be through a dedicated management network interface which is not physically accessible from the virtual machines. These interfaces should be isolated using ACL-controlled layer 3 measures.
    - An acceptable and equivalent level of security can be achieved by two virtual switches where the virtual machine technology in use supports this.
- Virtual storage systems must isolate Diageo data and metadata 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.

1.10 Remote Access

- Remote access must be restricted based on privilege.
- Only approved client builds can be used for remote access to the Diageo network.

- Persistent remote connections must use point-to-point VPN connections using approved cryptography mechanisms (e.g., IKEv2).
- All third party remote access for technical and support purposes must use approved software and access mechanisms. Exceptions must be approved by IM&S.
- Remote access connections, and hosts, must comply with Diageo's Access Management Standard, Privileged Access Management Standard and Firewall Policy.

Audience

This document is aimed at:

- Global Information Management & Security (IM&S).
- Technical staff involved in the commission, architecture, installation and change control of computer systems.
- Facilities.

Scope

This standard applies to all systems managed by or on behalf of Diageo as part of the network and systems infrastructure. This includes systems hosted on third party premises and managed as part of the Diageo network.

Objectives

This document serves as a standard for network and system design, architecture, configuration, and monitoring.

References

Access Management Standard
Authentication Standard
Cryptography Standard
Firewall Policy
Privileged Access Management Standard
Threat and Vulnerability Management (TVM) Standard

Exceptions

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

Incident Reporting

Any failure to comply with this document or security incident that materialises relating to the requirements within this standard must be reported to the Diageo Computer Security Incident (CSI) team by email at CSI@Diageo.com. Physical security incidents involving loss or theft of assets should be submitted through Diageo's ticketing system.

Document History

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	16th April 2018	Date of next review	13th May 2018

Version Number	Revision Date	Change History	Changes Marked	Updated By
2.8.1	16/04/2018	Very minor changes only in last bullet at 1.3, and 1.5 that references have been added specifically to personal information.	N/A	Tamas Sziller
2.8	10/07/2017	Clarity was given about encryption requirements to information/files transmission from/to outside and within Diageo: (i.e.: Confidential or Highly Confidential information must be always encrypted at rest and when in transit). Also many wording changes were made in order to achieve more precision.	N/A	Paul Galbraith / Tamas Sziller
2.7	06/12/2016	Updated section 1.5 Network and Access Segregation (Clarified network segregation)	Y	Paul Galbraith / Tamas Sziller
2.6	26/09/2016	Finalised Published Standard	N	Paul Galbraith
2.5	05/09/2016	Significant re-write of entire standard as part of the full PSG review & update process	N	Paul Galbraith
2.3	01/10/2015	Updated/added sections 3.1.5, 3.1.17, 3.2.4, 3.2.7, 3.4.7, 3.10.7, 3.10.8, 3.11.27, 3.11.28 as per D. Pendic recommendations	Y	Tamas Sziller
2.2	17/07/2015	Updated hyperlinks and removed 3.12.6 (IP phone network config detail) Added 3.4.8: Diageo and its vendors should have procedures in place for	Y	J. Haren / G. Duffy

		collecting evidence in line with local forensic evidence rules		
2.1	10/11/2014	Updated to new Standard Template. Added section 3.10.7, 3.10.8 and 3.11.27	N	J.Haren / D.Pendic
2.0	14/11/2013	Updated every section with extensive changes based on reviewers' input. Added in new standard structure at start of document	Y	J.Haren
1.0	10/08/2013	Document Issued	N	D.Pybus

Reviewers

This document requires to be reviewed by the following reviewers.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	May 2017
John Merritt	Global Information Security Director	May 2017
Paul Galbraith	Information Security Incident Prevention and Response Analyst	May 2017
Keith M Blair	SAP Technology Lead,	May 2017
Addleshaw Goddard	External legal counsel	April 2018
Stuart D. Holmes	Global Security Engineering and Ops Lead	May 2017
Brendan Fedigan	Solution Architect NAM, IS Service (EA)	Aug 2016
Ryuji Mori	Network Architect (EA)	May 2017
David Johnston	Lead Solutions Architect (EA)	Aug 2016

Approvers

This document requires the following approvals.

Name	Title	Approved Date
John Haren	IM&S Head of Governance, Risk & Compliance	11/04/2018

Distribution List

Once complete, this document will be distributed to:

Title (including company)
Above Approver List
IM&S Yammer Community
A&E Team
Global Operations & Engineering

End of Document