IS Audit Logging and Monitoring Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	13/09/2019
V 1.0	Andrew Clarke	Approved PWG	07/10/2019
	Andrew Clarke	Annual review	08/06/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 07 Oct 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 07 Oct 2019
Distribution:	

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering IS Audit and Event Logging and the Monitoring of log and Clock Synchronisation.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Systems Manager	Is responsible for maintaining and managing event logging and for clock synchronisation on IS server infrastructure
Network Manager	Is responsible for maintaining and managing event logging and for clock synchronisation on IS network infrastructure
College IT	Responsible for maintaining and managing event logging and for clock synchronisation on all College infrastructure
Cyber & Information Security Manager	Is responsible for ensuring security information and event management (SIEM) application compliant with Policy and reporting consistent with Policy

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A12 – Operations Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.12.4 - Logging and Monitoring

1.4 Scope

The scope of this policy applies to:
All of the University's servers and network infrastructure are within scope of this Policy

1.5 References

2.0 Event Logging and Monitoring Policy

2.1 Procedure

2.1.1. The Organisation uses a combination of software for complete monitoring, auditing and alerting of all its networks, services and users

2.1.2. Exabeam SIEM and Solarwinds Log Event Manager have been deployed and are in operation

2.2 Event logs recording user access and actions/activities, exceptions, faults and information security events shall be produced and kept for the minimum duration of 90 for all IS assets. (SIEM)

2.2.1 System administrators are prohibited from erasing or de-activating logs of their own activities.

2.2.2 Audit logs and the audit log reports are classified as University Confidential information and must be handled in line with the requirements of this ISMS for handling such information

2.3 Monitoring

2.3.1 Monitoring logs/reports are reviewed weekly. Any evidence of system misuse is reported to the Head of Infrastructure & Information Security who investigates further, and the disciplinary process may be invoked.

2.3.2 All systems and information assets being monitored must provide real-time alerting

2.4 These event logs must be protected to deny removal or modification by unauthorised persons.

2.4.1 Event logs and logging servers are restricted to authorised IS/Security staff only. Rules that only permit deletion and modification of these logs by authorised persons shall be applied.

2.4.2 Disabling audit logs or tampering with audit log information is treated as gross misconduct and the disciplinary policy may be invoked resulting in immediate dismissal.

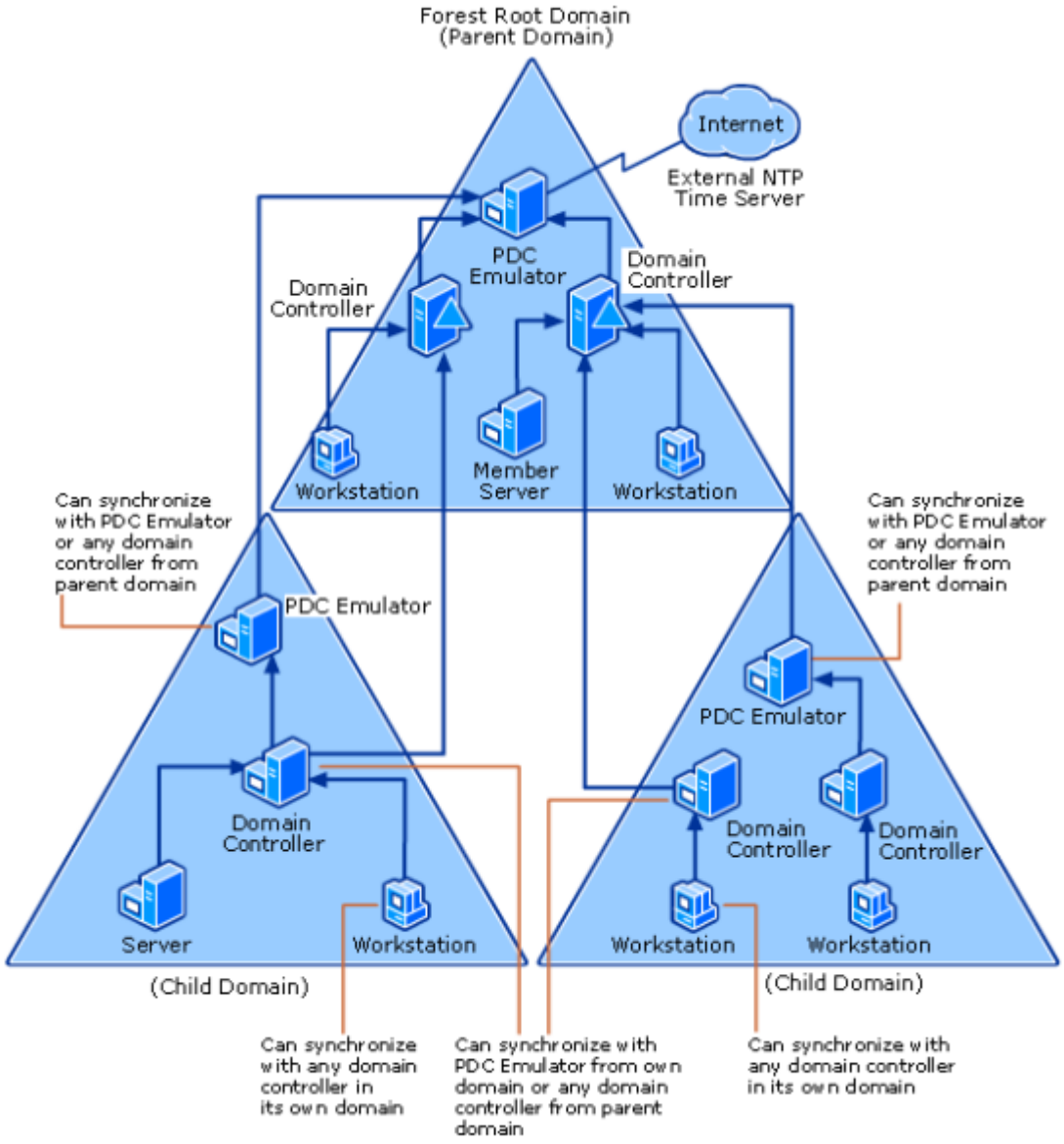
2.4.3 System logs are backed up in line with the ISMS Backup and restore Policy.

2.5 All Administrator and operator actions/activities shall be logged regardless of the privileges that they have on the systems and be made available for reporting and audits.

2.6 All systems should be configured to enable clock synchronisation in an automated manner with time servers from a single time source with the same time and date to facilitate incident traceability testing.

2.6.1 External NTP source (Stratum Level 2)
2.6.2 External firewall (Stratum Level 3) configured to synchronise time with external NTP source
2.6.3 All external networked appliances (Stratum Level 4) are configured to synchronise time with external firewall
2.6.4 Internal firewall (Stratum Level 4) configured to synchronise time with external firewall
2.6.5 All internal (Stratum Level 5) networked appliances are configured to synchronise time with internal firewall
2.6.6 Windows Domain Synchronisation
2.6.6.1 The PDC Emulators (Stratum Level 3) in each Forest Root Domain are configured to synchronise time with external NTP source
2.6.6.2 Time synchronisation for all other windows devices follows the 'Domain Hierarchy-Based Synchronisation' as per the diagram FIG 1
2.6.7 All other University devices (Linux, Unix) are configured to synchronise time with internal firewall

FIG 1


Forest Root Domain
(Parent Domain)
Internet
External NTP
Time Server
PDC
Emulator
Domain
Controller
Domain
Controller
Workstation
Member
Server
Workstation
Can synchronize
with PDC Emulator
or any domain
controller from
parent domain
PDC Emulator
Domain
Controller
Server
Workstation
(Child Domain)
Can synchronize
with PDC Emulator
or any domain
controller from
parent domain
PDC Emulator
Domain
Controller
Domain
Controller
Workstation
Workstation
(Child Domain)
Can synchronize
with any domain
controller in
its own domain
Can synchronize with
PDC Emulator from own
domain or any domain
controller from parent
domain
Can synchronize with
any domain controller
in its own domain