Document Control
Reference: BUL-POL-12.5.1
Issue No: 4
Issue Date: 22/06/2020
Page: 1 of 8

Standard Build Security Configurations 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	15/01/2018
V 0.2	Andrew Clarke	Amendments from Systems - Peter Polkinghorne	07/02/2018
V 1.0	Andrew Clarke	CISA Approval	07/09/2018
V 1.1	Andrew Clarke	Clarification on EOL Operating Systems (Point 2.1)	22/06/2020

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.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

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 Operating Systems security controls.

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
Head of Infrastructure & Operations	Is responsible for ensuring that server and network configurations are in line with the security requirements of the ISMS.
Systems Manager	Is responsible for maintaining and managing Operating systems on IT systems and infrastructure and ensuring that IS Operating systems comply with this policy.
Network Manager	Is responsible for maintaining and managing Operating systems on network systems and infrastructure comply with this policy.
Cyber & Information Security Manager	Is responsible for ensuring Operating system policy best practice and ensuring compliance with legislative and regulatory requirements.

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.12.5.1 Operating Systems Security

1.4 Scope

The scope of this policy applies to:

All of the University's servers are within scope of this Policy

1.5 References

CIS Benchmarks

1.6 Policy Objectives

The purpose of this policy is to provide guidance for the security of operating systems like Linux and Microsoft Windows, and its effect to the overall security of Web based applications and services. Based on the CIS's trusted computer system model, the current effort toward development of secure operating systems is defined.

This policy document sets out principles and expectations about when and how the Operating systems should (or should not) be configured.

2.0 Policy

Hardware & Virtualisation

The specification for Servers, both physical hardware and virtual, must exceed the recommended minimum requirements supplied by the manufacturer of the operating system intended to/or running on the asset;

Each server has a valid maintenance contract with the supplier, details of which are logged and includes; the asset/maintenance tag, Original ship date, level of support, contract renewal date and period of contract;

2.1 Operating Systems

- Server Operating Systems can only be installed by authorised systems administrators;
- Operating systems shall be installed and configured in-line with the manufacturers recommended installation guidance;
- Operating systems for Production, Test and Development systems should not run EOL (End of Life) or OOS (Out of Support) versions as per manufacturers recommendations;
- Operating systems shall have the University standard build installed comprising minimum components needed for operational purposes;
- Operating systems requiring a non-standard build for specific purposes/applications shall be installed comprising minimum components needed for operational purposes;

2.2 Applications

- Back Office Server Applications can only be installed by authorised systems administrators;
- Software shall be installed using a minimal installation making sure there are no code samples of demo files installed with the applications;
- Where necessary refer to the software vendors' guide for installation and security configuration best practices;

2.3 End-point AV & Malware

- End-point AV / Malware shall be installed on all of the Windows Organisations Servers (Linux servers are exempt from AV requirements);
- End-point AV / Malware shall be installed, updated & monitored from a central location;
- The software (including clients and server) shall automatically check for updates and update itself at least once per day;
- End-point AV / Malware shall provide real-time detection, correction and alerting functionality;
- Users shall be prevented from altering or stopping the configuration or status of the End-point AV / Malware;
- Versions of software which connect to the Organisations networks remotely shall be checked for compliance (latest version of agent, applications, policies, definitions) and is configured to quarantine connecting assets which

do not meet the required levels. They are placed in quarantine whilst they are automatically updated then permitted onto the network once complete;

2.4 Local Firewall

- All Servers shall be configured with the Firewall enabled;
- Modifications to the default domain policy are configured through Group Policy;
- Firewalls will be configured with both inbound and outbound rules. Any – Any rules are not permitted;
- The firewalls will be configured to permit services inbound or outbound which are essential to the normal operations for network, operating system, applications and management traffic;
- Users shall be restricted from stopping, modifying or overriding any of the Firewalls settings;

2.5 Vulnerability Management

- Automated Vulnerability Management security software shall be deployed to all Servers, desktops and laptops;
- Vulnerability Management software shall be installed, updated & monitored from a central location;
- The software (including clients and server) shall automatically check for updates and update itself at least once per day;
- An initial vulnerability assessment scan shall be performed on all desktops / laptops and any anomalies corrected before the information asset is moved into production
- Automated scheduled scans shall then run once every three months to ensure on-going compliance;

2.6 Host Intrusion Prevention System

- A Host Intrusion Prevention System shall be installed on all of the Organisations Servers, laptops & desktops;
- A Host Intrusion Prevention System shall be installed, updated & monitored from a central location;
- The software (including clients and server) shall automatically check for updates and update itself at least once per day;
- The Host Intrusion Prevention System shall provide real-time detection and interception of Malware and unknown threats prior to execution or during execution;
- Alerts for all incidents shall be configured to immediately inform the IS/Cyber Security teams;
- Users shall be prevented from altering or stopping the configuration or status of the Host Intrusion Prevention System software;

2.7 Hardening

- Servers and Applications shall be hardened in order to remove all unwanted operating system components, applications, services; (Ref 2.1 and 2.2)
- Access control lists and registry keys will have their base permissions restricted;

- Brunel University uses guidance and baselines from CIS (Centre for Internet Security) & Microsoft for the hardening of Microsoft operating systems;
- Brunel University uses guidance and baselines from CIS (Centre for Internet Security) for the hardening of Linux operating systems;
- Brunel University uses guidance and baselines from CIS (Centre for Internet Security) & Apple for the hardening of Apple iOS operating systems;
- All modifications, settings and configurations are saved within templates that are deployed automatically using Group Policy through Active Directory;
- Vulnerability Assessment software is scheduled to run periodically to test compliance;

2.8 Monitoring

- All Windows servers are monitored for patch management, software distribution, operating system deployment, network access protection and hardware and software inventory using SCCM and WSUS, Linux Servers are monitored using SMT & Satellite;

2.9 Backup

- Information is backed up during the server backup processes; DOC 12.3.1 - PROC - Backup and replication procedure