UNIVERSITY OF ABERDEEN

Digital and Information Services

Patch Management Policy

Patch Priority Schedule

Version 1.1 – September 2019

Document Control

File Name	Patch Priority Schedule.DOCX
Document Version	1.1
Document Owner	M. Marooth
Date Released	[Publish Date]
Readership	Digital and Information Services Operational and Support Teams. System Owners and Service Owners
Location	[SharePoint][Policy Zone]

Amendment History

Version	Date	Comment	Author
1.0	10th December 2018	Initial draft	M Marooth
1.1	20th September 2019	Contact Updates & Publish	M Marooth

Review and approvals

Function	Name	Date
Reviewed:	Distribution List	
Approved:	Information Governance Committee	June 2019

Distribution

Role	Name
Director of IT	Brian Henderson
CISO	Via IT Security Team
IT Security Manager	Garry Wardrope
Assistant Director (Service Management)	Richard Lynch
Assistant Director (Applications Management)	Ian Robotham
Infrastructure Manager	Derek Dawson
Network Manager	Alastair Matthews
Desktop Manager	Ian Rowley
Data Centre Manager	Martin Fraser
Service Desk Manager	Iain Cameron
Research IT Manager	Katie Wilde

CVSS Patch Priority

Patch Priority	Priority Schedule	Comments
Security	Within 14 days of Release	As assessed locally
Critical	Within 14 days of Release	CVSS Score 9.0 – 10.0
High	Within 14 days of Release	CVSS Score 7.0 – 8.9
Medium	Within 30 days of Release	CVSS Score 4.0 – 6.9
Low	Within 90 days of Release	CVSS Score 0.01 – 3.9
None	As time permits	CVSS Score 0.00

Patch Assessment Matrix

Metric	Condition/Status	Priority
Attack Vector	Local Network	Critical
	Adjacent Network	High
	Local Environment	Medium
	Physical Environment	Low
Attack Complexity	Low – Easy to Exploit	Critical
	High – Difficult to Exploit	Low
Privilege Required	None	Critical
	Basic	High
	Authorization	Medium
User Interaction Required	None	Critical
	Required	High
Scope	Localised	Medium
	Widespread	Critical
Data Loss Impact	Confidential/Personal/Financial	Critical
	Private/Institutional	High
	Public	Medium
	None	Low
Service/System Availability	Unavailable	Critical
	Reduced Performance	High
	No Impact	Low
Exploit Maturity	High	Critical
	Functional	High
	Proof of Concept	Medium
	None Known	Low
Report Confidence	Confirmed	Critical
	Reasonable	High
	Unconfirmed	Medium
	Unknown	Low
Service Priority	0	Critical
	1	High
	2	Medium
	3	Low

Title	Vulnerability & Patch Management Policy
Author / Creator	Mark Marooth
Owner	Garry Wardrope IT Security Manager
Date published / approved	Approved June 2019 Published September 2019
Version	1.7
Date for Next Review	September 2020
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University and have responsibility for ensuring that IT Systems are patched.
Related	Conditions for using IT Facilities Information Security Policy Cyber Essentials +
Subject / Description	Purpose of this policy is to ensure that all University of Aberdeen IT Infrastructure is properly maintained and patched to minimise vulnerabilities and ensure the confidentiality, integrity and availability of the IT Infrastructure.
Equality Impact Assessment	N/A
Section	Digital and Information Services
Theme	IT Infrastructure Protection
Keywords	IT Infrastructure, Vulnerability, Patch, Vulnerability & Patch Management, Patch Schedule, Compliance, CVSS