Information Security – Threat and Vulnerability Management Procedure

Intent

The intent of this Procedure is to establish a clear and efficient process for managing system vulnerabilities, ensuring the security and resilience of James Cook University's (JCU; the University) digital technology assets.

Scope

This Procedure applies to all Authorised Users of the University's information management systems regardless of location, whether during or after business hours or whether on JCU-owned or JCU managed devices.

Definitions

Refer to the Digital Policy Glossary for a comprehensive list of definitions, terms and explanations relating to information security at JCU.

Business Owner - Is the primary stakeholder for a digital technology asset, and the role responsible for defining business objectives and making high-level decisions about the asset. They ensure the asset aligns with organisational strategy and complies with relevant policies and regulations.

Product Owner - The role responsible for managing the technical aspects of a digital technology asset (product), ensuring its alignment with IT standards and architectures. The Product Owner oversees the asset's security, reliability, and efficiency throughout its lifecycle, working closely with the Business Owner to align technology solutions with business needs.

System Manager – The role responsible for ensuring the day-to-day system availability, reliability, and performance. The System Manager coordinates daily management of the asset, including monitoring performance, maintenance, upgrades, and troubleshooting.

Vulnerability – is a weakness or flaw in a digital technology asset that can be exploited by threats to gain unauthorised access or cause harm. They can arise from various sources, including software bugs, misconfigurations, or inadequate security practices.

Introduction

In this procedure:

- Vulnerability includes both potential and actual vulnerabilities.
- Vulnerability scanning is performed on computers, servers, network devices, and other hardware, as well as the systems and environments where software is installed and run. While software is a crucial part of these assets the focus is on the system rather than scanning individual pieces of software. JCU uses the Common Vulnerability Scoring System version 3 (CVSSv3) risk rating to assign a score to each vulnerability based on factors such as exploitability, impact, and complexity. This aids in prioritising remediation efforts. Table 1 specifies the maximum risk assessment and remediation timeframes for each risk rating.

Table 1: Vulnerability Risk Assessment and Remediation Timeframes

CVSSv3 Risk Rating	External Facing	Personal Information	Restricted Data Classification	Maximum Timeframe to Assess Risk *(Upon Notification)*	Maximum Timeframe to Remediate Vulnerabilities *(Upon Notification)*	JCU Risk Rating
Critical	Yes	N/A	N/A	Four (4) business hours	Two (2) business days	Catastrophic
	No	Yes	N/A	Four (4) business hours	Two (2) business days	Catastrophic
	No	No	Yes	Four (4) business hours	Two (2) weeks	Major
	No	No	No	Four (4) business hours	Two (2) weeks	Major
High	Yes	N/A	N/A	One (1) week	Two (2) weeks	Major
	No	Yes	N/A	One (1) week	Two (2) weeks	Major
	No	No	Yes	One (1) week	One (1) month – managed via automatic patching	Moderate
	No	No	No	One (1) month	One (1) month – managed via automatic patching	Moderate
Medium	Yes	N/A	N/A	One (1) month	One (1) month – managed via automatic patching	Moderate
	No	Yes	N/A	One (1) month	One (1) month – managed via automatic patching	Moderate
	No	No	No	One (1) month	One (1) month – managed via automatic patching	Minor
Low	Yes	No	Yes	One (1) month	One (1) month – managed via automatic patching	Minor
	N/A	N/A	N/A	One (1) month	One (1) month – managed via automatic patching	Insignificant

Important Information:
Any deviation from this table (e.g., for research assets such as MARF life support systems or lab instruments, where patching could cause intolerable downtime) requires approval from the Information and Cybersecurity Manager. This approval must be documented, retained, and understood (e.g., through a security assessment process, a ServiceNow request, a change management process, or another appropriate method). The Information and Cybersecurity Manager will assess each request and, if necessary, advise the Information Security – Governance, Risk, and Compliance (GRC) Manager to add the deviation to the Information Security Risk Register. It is important to note that responsibility for managing the risk does not reside with these managers; their role is to triage and escalate the risk as appropriate.

Procedure

*Refer to the **Information Security – Threat and Vulnerability Management Standard** for specific requirements that align with this procedure.*

Table of Contents

1. Identifying and Managing JCU's Digital Technology Assets

Action		Responsible Officer
1.1	Review, understand and adhere to the requirements outlined in ***Table 1: Vulnerability Risk Assessment and Remediation Timeframes.***	• Product Owners • Information and Cybersecurity Manager • GRC Manager
1.2	Ensure all new and existing digital technology assets are provisioned, maintained and configured for scanning by JCU's vulnerability management solution by using automatic processes or by submitting a ServiceNow Request.	• Product Owners
1.3	Ensure Third-Party Service Providers engaged by JCU to manage external services are aware of the requirements of this procedure, particularly the timeframes contained within **Table 1: Vulnerability Risk Assessment and Remediation Timeframes**	• Product Owners

2. Scanning for Vulnerabilities

Action		Responsible Officer
2.1	Actively monitor and assess both the internal and external attack surface to identify and address potential weaknesses or threats in JCU's systems and networks.	• Information and Cybersecurity Manager
2.2	Automate regular vulnerability scans on all digital technology assets and across all attack surfaces using JCU's vulnerability management solution.	• Information and Cybersecurity Manager
2.3	Schedule and manage the deployment of vulnerability scans following any significant change in the network and for any new system components being deployed to JCU's enterprise or operational environment.	• Information and Cybersecurity Manager
2.4	Ensure vulnerability scanning results are stored in a secure environment, accessible only to Authorised Users.	• Information and Cybersecurity Manager

3. Actions Upon Discovering a Vulnerability

Action		Responsible Officer
3.1	*Low and Medium Vulnerabilities* • If a patch is available, no further action is required as the vulnerability will be automatically patched.	• Information and Cybersecurity • Product Owners
3.2	*High or Critical Vulnerabilities* Create a ServiceNow Incident and notify the following parties within 48 hours of becoming aware of any high or critical rated vulnerabilities affecting assets that contain and/or manage JCU-owned data: • Information and Cybersecurity Manager • Business Owner • Product Owners	• Information and Cybersecurity • Product Owners
3.3	Assess the vulnerability to determine JCU's risk rating. • Collaborate with the relevant Product Owners and other stakeholders where necessary. • Use Table 1: Vulnerability Risk Assessment and Remediation Timeframes, to assess the technical severity, potential impact, exploitability and strategic significance.	• Cybersecurity Analyst • Information and Cybersecurity Manager • Product Owners
3.4	Submit a ServiceNow Incident and document the tasks necessary to mitigate the risk. • Patching is a critical method for remediation and risk mitigation - refer to Section 4 Patch Management for further guidance.	• Cybersecurity Analyst • Information and Cybersecurity Manager
3.5	Execute the tasks identified in ServiceNow to mitigate the risk. • If Third-Party Service Providers are responsible for actioning these tasks, ensure appropriate communication and coordination. • Notify the Cybersecurity Team of progress and any issues that arise, as appropriate.	• TS Staff • Product Owners

3.6	Liaise with the risk owner, usually the Business Owner, to determine if the risk can be accepted without remediation in its current state or due to a lack of mitigating controls. If: • Yes - Document the risk in the Information Security Risk Register in collaboration with the Information Security – Governance Risk and Compliance (GRC) Manager. Continue to Step 3.9. • No – Treat the risk by adding compensatory controls as mitigating measures and advise the Information and Cybersecurity Manager.	• Product Owners • Business Owners
3.7	Develop a plan for compensatory controls e.g., reconfiguration, isolation, or removal of the digital technology asset or service.	• Information and Cybersecurity Manager • Product Owners
3.8	Seek approval from both the Chief Digital Officer (CDO) and the Business Owner to implement compensatory controls. • If approved - Add tasks for compensatory controls to the Information Security Risk Register, with the Business Owner recorded as the formal risk owner. • If not approved – The CDO and the Business Owner or an appropriate senior authority (such as a member of the Senior University Leadership), will need to formally accept this as a risk in the Information Security Risk Register, with the Business Owner recorded as the formal risk owner.	• Information and Cybersecurity Manager • Product Owners
3.9	Keep the Chief Information Security Officer (CISO) informed about remediation efforts for vulnerabilities with a catastrophic and major risk rating.	• Information and Cybersecurity Manager
3.10	Keep Senior University Leadership informed about remediation efforts for vulnerabilities with a catastrophic and major risk rating.	• CISO
3.11	Monitor ServiceNow to ensure tasks are being completed within specified timeframes and escalate issues as required.	• Information and Cybersecurity Manager

4. Patch Management

Action		**Responsible Officer**
4.1	Maintain active subscriptions for vendor support to ensure access to updates, technical assistance, and compliance with licensing agreements.	• Product Owners
4.2	Ensure the digital technology asset is configured and maintained in an approved central configuration and patch management system e.g., SCCM/MECM or Red Hat Satellite.	• Product Owners
4.3	Test, verify and deploy patches and supplementary configurations using an automated workflow through a central software and configuration management platform. • This includes provisioning the asset for management and establishing a like-for-like testing environment (where available) for patches to simulate actual system conditions. • Research systems may require special consideration around deployment to accommodate particular functions e.g., long-	• Product Owners

Action		Responsible Officer
	running processes that cannot be impacted by a system restart.	
4.4	Liaise with the Information and Cybersecurity Manager on any issues encountered that affect compliance to remediation timeframes.	• Product Owners
4.5	Enter any related change requests in ServiceNow and ensure the successful application of patches by Third-Party Service Providers, documenting progress on their behalf.	• Product Owners

5. Verification and Validation of Remediation

Action		Responsible Officer
5.1	Manage the verification and validation process, collaborating with Product Owners and Third-Party Service Providers where appropriate.	• Information and Cybersecurity Manager
5.2	Conduct post-remediation testing to verify and validate the effectiveness of applied patches and updates.	• Product Owners
5.3	Provide updates on progress and report any issues to System Managers and the Information and Cybersecurity Manager.	• Product Owners
5.4	Update incident tasks in ServiceNow, including updates on behalf of Third-Party Service Providers.	• Product Owners
5.5	Collaborate with business teams to validate that system functionality and business processes are working as expected post-remediation.	• Product Owners
5.6	Advise the Information and Cybersecurity Manager and relevant stakeholders of any issues of concern arising during the verification and validation process.	• Product Owners
5.7	Report progress on the verification and validation process for major or catastrophic risks to the CISO.	• Information and Cybersecurity Manager
5.8	Keep Senior University Leadership informed about any verification and validation efforts that prove non-effective for major or catastrophic risks.	• CISO

6. Penetration Testing

Action		Responsible Officer
6.1	Manage the internal and external penetration testing process, ensuring appropriate activities do not adversely impact system performance or data integrity.	• Information and Cybersecurity Manager
6.2	Support the Information and Cybersecurity Manager by assisting in testing scheduling and providing technical support and information as required.	• Product Owners

Action		Responsible Officer
6.3	After initial penetration testing, follow-up tests will be conducted to confirm that all identified vulnerabilities have been effectively remediated.	• Product Owners
6.4	Advise the Information and Cybersecurity Manager and relevant stakeholders of any issues of concern arising during penetration testing.	• Product Owners
6.5	Report progress on the testing process to the CISO.	• Information and Cybersecurity Manager
6.6	Keep Senior University Leadership informed about any major or catastrophic issues.	• CISO
6.7	Ensure penetration testing results are encrypted and stored in a secure environment, accessible only to authorised users.	• Product Owners

7. Exception and Exemption Management

Action		Responsible Officer
7.1	Upon notification, document, and manage any exceptions or exemptions to this procedure in the Information Security Risk Register. This includes: • Triaging the exceptions to determine the level of risk. • Seeking approval from the appropriate senior authority. • Documenting and communicating outcomes to stakeholders. • Monitoring and reviewing the exceptions or exemptions periodically to ensure continued relevance and appropriateness.	• Information Security – GRC Manager

8. Consequence Management

Action		Responsible Officer
8.1	Implement an Incident Response Plan for any security incident or breach resulting from a failure in patching or a vulnerability.	• Information and Cybersecurity Manager

9. Continuous Improvement and Compliance

Action		Responsible Officer
9.1	Continuously monitor, analyse, and assess: • JCU's attack surface to verify accuracy and completeness • Vulnerability scanning tools, tracking, and ticketing systems to verify accuracy, efficiency, and completeness.	• Information and Cybersecurity Manager
9.2	Create tasks in ServiceNow to record and manage actions required from reviews.	• Information and Cybersecurity Manager

Action		Responsible Officer
9.3	Manage persistent non-adherence and/or critical security issues related to this procedure following JCU's Code of Conduct and relevant HR processes.	• Information and Cybersecurity Manager • Information Security - GRC Manager
9.4	Develop monitoring mechanisms and perform regular reviews to ensure compliance with government legislation and reporting. • Ensure gaps and non-compliance issues are promptly addressed and remediated.	• Information and Cybersecurity Manager

10. Monitoring Cloud Security

Action		Responsible Officer
10.1	Monitor cloud computing provider security dashboards to identify and address deviations from vendor best practices. • The frequency of review should consider any significant events, security incidents, compliance requirements and maintaining a proactive security posture.	• Information and Cybersecurity Manager • Product Owners

11. Reporting

Action		Responsible Officer
11.1	Provide monthly reports to CISO, Product Owners and CDO, including: • Status of vulnerabilities and remediation actions. • Trends or systemic issues that may require adjustments to existing procedures and processes. • Close-out rates in ServiceNow for tasks related to vulnerability and patch management. • Outcomes from audits and reviews. • Threat intelligence insights and recommendations for improvement.	• Information and Cybersecurity Manager
11.2	Provide updates to relevant committees e.g., Vice Chancellor Committee, Research Committee. Deputy Vice Chancellor – Research Advisory Committee, etc, as appropriate.	• CISO

Related Policy Instruments

Digital Technologies Acceptable Use Policy

Digital Technologies Acceptable Use Procedure

Queensland Government Information Security Policy (IS 18:2018)

ISO/IEC 27001 Information security, cybersecurity, and privacy protection – Information security management systems – Requirements

ISO/IEC 27002 Information security, cybersecurity, and privacy protection – Information security controls.

Information Security Management Framework

Information Security Policy

Schedules/Appendices

N/A

Administration

NOTE: Printed copies of this procedure are uncontrolled, and currency can only be assured at the time of printing.

Approval Details

Policy Domain	Corporate Governance
Policy Sub-domain	Risk, Assurance, Regulatory and Compliance
Policy Custodian	Vice Chancellor
Approval Authority	Council
Date for next Major Review	25/10/2029

Revision History

Version	Approval date	Implementation date	Details	Author
24-1	25/10/2024	30/10/2024	Procedure established to support the Information Security Policy.	Information and Cybersecurity Manager

Keywords	Patch management, security controls
Contact person	Information Security - Governance, Risk and Compliance Manager