Information Security Operations Management Procedure

THE UNIVERSITY OF NEWCASTLE AUSTRALIA

A. Procedure

1. Audience

1.1 All University staff, vendors, students, volunteers, and members of advisory and governing bodies, in all campuses and locations of the University and at all times while engaged in University business or otherwise representing the University

2. Executive Summary

2.1 The University of Newcastle is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

2.2 All users interacting with information assets have a responsibility to ensure the security of those assets.

2.3 The University must have controls in place to ensure the smooth operation of the University's ICT Resources. Users must be trained, equipped and periodically reminded to use information and associated infrastructure securely.

B. Operational Procedures and Responsibilities

Objective: To ensure correct and secure operations of information systems

1. Documented Operating Procedures

1.1 Operating procedures and responsibilities for information systems must be authorised, documented and maintained.

1.2 Information Owners and System Owners must ensure that Standard Operating Procedures (SOP) and standards are:

(a) documented;

(b) approved by the appropriate authority;

(c) consistent with University policies;

(d) reviewed and updated periodically;

(e) reviewed and updated when there are changes to equipment/systems or changes in business services and the supporting information systems operations; and

(f) reviewed and updated following a related security incident investigation.

1.3 The documentation must contain detailed instructions regarding:

(a) information processing and handling;

(b) system restart and recovery procedures;

(c) backup and recovery including on-site and off-site storage;

(d) exceptions handling, including a log of exceptions;

(e) output and media handling, including secure disposal or destruction;

(f) Management of audit and system log informaiton;

(g) change management including scheduled maintenance and interdependencies;

(h) computer room management and safety;

(i) Information Incident Management Process;

(j) Disaster Recovery;

(k) Business Continuity Plan; and

(l) contact information for operations, technical, emergency and business personnel.

2. Change Management

2.1 Changes to business processes and information systems that affect information security must be controlled.

2.2 All changes to the University's ICT services and systems environment, including provisioning and de-provisioning of assets, promotion of code, configuration changes and changes to Standard Operating Procedures must be authorised by the University IT Change Advisory Board (CAB).

2.3 The change management process must follow the guidelines, approvals and templates provided as per the University Transition Process.

2.4 Changes must be controlled by:

(a) identifying and recording significant changes;

(b) assessing the potential impact, including that on security, of the changes;

(c) obtaining approval of changes from those responsible for the information system;

(d) planning and testing changes including the documentation of rollback procedures;

(e) communicating change details to relevant personnel, Users and stakeholders; and

(f) evaluating that planned changes were implemented as intended.

2.5 Information Owners and System Owners must plan for changes by:

(a) assessing the potential impact of the proposed change on security by conducting a security review and a Threat and Risk Assessment;

(b) identifying the impact on agreements with business partners and external parties including information sharing agreements, licensing and provision of services;

(c) preparing change implementation plans that include testing and contingency plans in the event of problems;

(d) obtaining approvals from affected Information Owners; and

(e) training technical of operational staff as necessary;

2.6 Information Owners and System Owners must implement changes by:

(a) notifying affected internal parties, business partners and external parties;

(b) following the documented implementation plans;

(c) training users if necessary;

(d) documenting the process throughout the testing and implementation phases; and

(e) confirming the changes have been performed and no unintended changes took place

3. Capacity Management

3.1 The use of information system resources must be monitored and optimised with projections made of future capacity requirements.

3.2 Information Owners and System Owners are responsible for implementing capacity management processes by:

(a) documenting capacity requirements and capacity planning processes;

(b) including capacity requirements in service agreements; and

(c) monitoring and optimising information systems to detect impending capacity limit.

3.3 Information Owners and System Owners must project future capacity requirements based on:

(a) new business and information systems requirements;

(b) statistical or historical capacity requirements; and

(c) current and expected trends in information processing capabilities (e.g. introduction of more efficient hardware or software).

3.4 Information Owners and System Owners must use trend information from the capacity management process to identify and remediate potential bottlenecks that present a threat to system security or services

4. Separation of Development, Testing and Production Environments

4.1 Development, testing and production environments must be separated to reduce the risks of unauthorised access or changes to the production environment.

4.2 Information Owners and System Owners must:

(a) separate production environments from test and development environments by using different servers, networks and where possible different domains;

(b) ensure that production servers do not host test or development services or applications;

(c) prevent the use of test and development identities as credentials for production systems;

(d) store source code in a secure location away from the production environment and restrict access to specified personnel;

(e) prevent access to compilers, editors and other tools from production systems;

(f) use approved change management processes for promoting software from development/test to production;

(g) prohibit the use of production data in development, test or training systems; and

(h) prohibit the use of sensitive information in development, test or training systems in accordance with the System Acquisition, Development and Maintenance Procedure

C. Protection from Malware

Objective: To ensure that information systems are protected against malware

1. Controls Against Malicious Code

1.1 Detection, prevention and recovery controls – supported by user awareness procedures – must be implemented to protect against malware.

1.2 Information Owners and System Owners must protect University information systems from malicious code by:

(a) installing, updating and using software designed to scan, detect, isolate and delete malicious code;

(b) preventing unauthorised Users from disabling installed security controls;

(c) prohibiting the use of unauthorised software;

(d) checking files, email attachments and file downloads for malicious code before use;

(e) maintaining business continuity plans to recover from malicious code incidents;

(f) maintain a critical incident management plan to identify and respond to malicious code incidents;

(g) maintaining a register of specific malicious code countermeasures (e.g. blocked websites, blocked file extensions, blocked network ports) including a description, rationale, approval authority and the date applied; and

(h) developing user awareness programs for malicious code countermeasures.

1.3 University IT Security staff are responsible for communicating technical advice and providing information and awareness activities regarding malicious code

D. Backup

Objective: To protect against loss of data

1. Information Backup

1.1 Backup copies of information, software and system images must be made, secured, and be available for recovery.

1.2 Information Owners and System Owners must define and document backup and recovery processes that consider the confidentiality, integrity and availability requirements of information and information systems.

1.3 Backup and recovery processes must comply with:

(a) University business continuity plans (if applicable);

(b) policy, legislative, regulatory and other obligations; and

(c) records management requirements (refer Records Management Policy).

1.4 The documentation for backup and recovery must include:

(a) types of information to be backed up;

(b) schedules for the backup of information and information systems;

(c) backup media management;

(d) methods for performing, validating and labelling backups; and

(e) methods for validating the recovery of information and information systems.

1.5 Backup media and facilities must be appropriately secure based on a security review or Risk Assessment. Controls to be applied include:

(a) use approved encryption;

(b) physical security;

(c) access controls;

(d) methods of transit to and from off-site locations;

(e) appropriate environmental conditions while in storage; and

(f) off-site locations must be at a sufficient distance to escape damage from an event at the main sitePrinciples

---

E. Log Management

Objective: To log events and monitor compliance

1. Event Logging

1.1 Event logs recording user activities, exceptions, faults and information security events must be produced, kept and regularly reviewed.

1.2 Information Owners must ensure that event logs are used to record user and system activities, exceptions and events (security and operational). The degree of detail to be logged must be based on the value and sensitivity of the information and the criticality of the system. The resources required to analyse the logs must also be considered. Where applicable, event logs must include:

(a) user ID;

(b) system activities;

(c) dates, times and details of key events (e.g. logon, logoff);

(d) device identity and location;

(e) logon method;

(f) records of successful and unsuccessful system access attempts;

(g) records of successful and unsuccessful data and other resource access attempts;

(h) changes to system configuration;

(i) use of elevated privileges;

(j) use of system utilities and applications;

(k) network addresses and protocols;

(l) alarms raised by the access control system;

(m) activation and de-activation of protection systems (e.g. anti-virus, intrusion detection); and

(n) records of transactions executed by users in applications.

1.3 Event logs may contain sensitive information and therefore must be safeguarded in accordance with the requirements of the section on the Protection of Log Information.

1.4 System administrators must not have the ability to modify, erase or de-activate logs of their own activities.

1.5 If event logging is disabled the decision must be documented. Include the name and position of the approver, date and rationale for de-activating the log.

1.6 Event logs may be configured to alert someone if certain events or signatures are detected. Information Owners and System Owners must establish and document alarm response procedures to ensure they are responded to immediately and consistently. Normally, response to an alarm will include:

(a) identification of the event;

(b) isolation of the event and affected assets;

(c) identification and isolation of the source;

(d) corrective action;

(e) forensic analysis;

(f) action to prevent recurrence; and

(g) securing of event logs as evidence

2. Protection of Log Information

2.1 Information system logging facilities and log information must be protected against tampering and unauthorised access.

2.2 Information Owners must implement controls to protect logging facilities and log files from unauthorised modification, access or destruction. Controls must include:

(a) physical security safeguards;

(b) permission for administrators and operators to erase or de-activate logs;

(c) multifactor authentication for access to highly-restricted records;

(d) backup of audit logs to off-site facilities;

(e) automatic archiving of logs to remain within storage capacity; and

(f) scheduling the audit logs as part of the records management process.

2.3 Event logs must be retained in accordance with the records retention schedule for the information system.

2.4 System logs for University critical IT infrastructure (P1 list) must be retained for at least 30 days online and archived for 90 days.

2.5 Datacentre physical access logs must be made available for at least 90 days and CCTV records must be retained for at least 30 days.

2.6 Logs must be retained indefinitely if an investigation has commenced or it is known that evidence may be obtained from them

3. Administrator and Operator Logs

3.1 Activities of privileged users must be logged and the log subject to regular independent review.

3.2 The activities of system administrators, operators and other privileged user must be logged including:

(a) the time an event (e.g. success or failure) occurred;

(b) event details including files accessed, modified or deleted, errors and corrective action taken;

(c) the account and the identity of the privileged user involved; and

(d) the systems processes involved.

3.3 Logs of the activities of privileged users must be checked by the Information Owner or delegate. Checks must be conducted regularly and randomly. The frequency must be determined by the value and sensitivity of the information and criticality of the

system. Following verification of the logs they must be archived in accordance with the applicable records retention schedule.

4. Clock Synchronisation

4.1 Computer clocks must be synchronised for accurate recording.

4.2 System administrators must synchronise information system clocks to the local router gateway or a University approved host.

4.3 System administrators must confirm system clock synchronisation following power outages and as part of incident analysis and event log review

---

F. Control of Operational Software

Objective: To ensure the integrity of production systems

1. Installation of Software on Production Systems

1.1 The installation of software on production information systems must be controlled.

1.2 To minimise the risk of damage to production systems Information Owners must implement the following procedures when installing software:

(a) updates of production systems must be planned, approved, assessed for impacts, tested and logged;

(b) a Change and Release Coordinator must be appointed to coordinate the install and update of software, applications and program libraries;

(c) operations personnel and end users must be notified of the changes, potential impacts and, if required, given additional training;

(d) production systems must not contain development code or compilers;

(e) user acceptance testing must be extensively and successfully conducted on a separate system prior to production implementation;

(f) a rollback strategy must be in place and previous versions of application software retained;

(g) old software versions must be archived with configuration details and system documentation; and

(h) updates to program libraries must be logged

G. Vulnerability Management

Objective: To prevent exploitation of technical vulnerabilities

2. Management of Technical Vulnerabilities

2.1 Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risk.

2.2 To support technical vulnerability management, Information Owners and System Owners must maintain an inventory of information assets in accordance with the Information Security Asset Management Procedure. Specific information must be recorded including:

(a) the software vendor;

(b) version numbers;

(c) current state of deployment; and

(d) the person(s) responsible for the system.

2.3 Vulnerabilities which impact University information systems must be addressed in a timely manner to mitigate or minimise the impact on University operations. The IT Security Team shall ensure that vulnerability assessments (VA) are conducted for the University's ICT services and systems on a regular basis.

2.4 Vulnerability remediation efforts, including patch implementations, shall be coordinated and processed according to the University's Patch Management Procedure and University Risk Management Framework.

2.5 All internal and external University ICT systems and resources are covered in this Procedure:

(i) Internal Vulnerability Assessments

(ii) Servers used for internal hosting and supporting Infrastructure

(iii) Servers which will be accessed through reverse proxy

(iv) Research specific servers and applications

(v) Research devices and systems

(vi) Desktops and workstations

(b) External Vulnerability Assessments

(i) Perimeter network devices exposed to internet

(ii) All external facing servers and services

(iii) Network appliances, streaming devices and essential IP assets that are internet facing.

(iv) Public facing research applications and devices

(v) Cloud based services

3. Vulnerability Management Cycle

3.1 Asset Discovery

(a) Asset Discovery scan will be executed on a monthly basis or quarterly on the segments to determine the live assets connected to the network.

(b) Network team will share the IP segments of all assets within the University including Datacentres and other Virtual LAN's with the IT Security Team.

(c) IT Security Team will perform an asset discovery scan on the segments.

(d) Any assets added or removed from the segment will be detected in the asset discovery scan.

(e) IT Security Team will share with Network team the addition/removal of servers/devices for reconfirmation based on the discovery scan.

(f) Final list of IP/IP Segments will be scanned for Vulnerabilities

3.2 Scan – Remediate – Rescan

(a) IT Security team shall perform Vulnerability Analysis Scan on all University Critical Infrastructure Servers on a monthly basis and non-critical assets on at least a quarterly basis.

(b) IT Security Team will perform a risk assessment to map the risk, threat, likelihood and impact rating for the vulnerabilities noted.

(c) The University Risk Management Framework shall be followed to perform the risk assessment.

(d) IT Security Team shall inform the System Owners regarding the results of the scans and share the vulnerability reports with the Responsible Administrators for each system.

(e) All vulnerabilities identified in the VA Scan shall be remediated by according to the Remediation timeline below (7.1.3).

(f) The System Owners shall inform IT Security Team regarding the completion of vulnerability remediation.

(g) Vulnerabilities that cannot be actioned within the defined timeframe will need an exception approved.

3.3 Ad-Hoc Scans

(a) Ad-hoc scans include scans on any new infrastructure devices/servers/services prior to production deployment as per the following process.

(i) New service owners shall complete a Service Desk request ticket and submit to the IT Security Team for actioning.

(ii) The IT Security Team shall perform Vulnerability Analysis Scan of specific systems (including servers) as per the environment and technology used for the system.

(iii) VA report shall be submitted to Business owner and respective System Owner or team.

(iv) IT Security Team lead will validate with respective System Owners on closure of all the vulnerabilities and then perform a rescan.

(v) Vulnerabilities that cannot be actioned within the defined timeframe will need an exception approved, with risk acceptance and compensating controls implemented and documented.

(vi) Assets / services / devices can be released to production only after the final sign off by IT Security Team

4. Classification of Vulnerabilities

4.1 Vulnerabilities are classified based on their impact in a given environment, to data/information or to the University's reputation

Rating	Red Hat[i], Microsoft[ii] & Adobe[iii] Rating	Typical CVSS[iv] Score	Description
Critical	Critical	10	A vulnerability whose exploitation could allow code execution or complete system compromise without user interaction. These scenarios include self-propagating malware or unavoidable common use scenarios where code execution occurs ***without*** warnings or prompts. This could include browsing to a web page or opening an email or no action at all.
High	Important	7.0 – 9.9	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. This includes common use scenarios where a system is compromised ***with*** warnings or prompts, regardless their provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered.
Medium	Moderate	4.0 – 6.9	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations. The vulnerability is normally difficult to exploit.

Low	Low	< 4.0	This classification applies to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.

5. Remediation Timeline and Risk Acceptance

5.1 All vulnerabilities identified in a VA Scan shall be addressed within the timeline described below. If any particular vulnerability cannot be remediated within this timeframe, the risk of data loss/attack on the device should be formally documented and accepted by the respective groups in below table. Remediation time and risk acceptance for the identified vulnerabilities shall be as follows:

Vulnerability Level	Remediation Timelines		Risk Acceptance
	External Facing Devices	Internal Devices	
Critical	1 Week	1 Week	CIO or Risk Management Office
High	2 Weeks	2 Weeks	CIO
Medium	3 Weeks	Next Maintenance Window	Information Owner
Low	Next Maintenance Window	Next Maintenance Window	Information Owner

6. Third Party Scans

6.1 A third party must be engaged annually to perform vulnerability assessment & penetration testing covering all internet facing University ICT services and systems and critical internal non-internet facing ICT services and systems.

7. Vulnerability Management Roles and Responsibilities

7.1 IT Security Team

(a) Perform asset discovery and performing Vulnerability Management Process

(b) Approve the Vulnerability Assessment Schedule

(c) Oversee vulnerability remediation.

(d) Targeting vulnerability program maturity through metrics development

(e) Monitor security sources for vulnerability announcements and emerging threats that correspond to the system inventory.

7.2 System Owners

(a) Responsible for implementing remediating actions defined as a result of detected vulnerabilities.

(b) testing and evaluating options to mitigate or minimise the impact of vulnerabilities;

(c) applying corrective measures to address the vulnerabilities; and

(d) reporting to the IT Security Team on progress in responding to vulnerabilities

7.3 Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the change management controls or by following the UoN Information Security Incident Management Guidelines.

7.4 Responsibilities for vulnerability response must be included in service agreements with suppliers.

8. Restrictions on Software Installation

8.1 Rules governing the installation of software by users must be established and implemented.

8.2 Users are not allowed to install software on University devices unless specifically authorised by a System Owner or a system administrator. System Owners are responsible for the installation of software, updates and patches.

H. Information Security Audit Considerations

Objective: To minimise the impact of audit activities on production systems

1. Information Systems Audit Controls

1.1 Audit requirements and activities involving checks on production systems must be planned and approved to minimise disruption to business processes.

1.2 Prior to commencing compliance checking activities such as audits or security reviews of production systems the CIO, and the Information Owner must define, document and approve the activities. Among the items upon which they must agree are:

(a) the audit requirements and scope of the checks;

(b) audit personnel must be independent of the activities being audited;

(c) the checks must be limited to read-only access to software and data, except for isolated copies of system files, which must be erased or given appropriate protection if required when the audit is complete;

(d) the resources performing the checks must be explicitly identified;

(e) existing security metrics will be used where possible;

(f) all access must be monitored and logged and all procedures, requirements and responsibilities must be documented;

(g) audit tests that could affect system availability must be run outside business hours; and

(h) appropriate personnel must be notified in advance in order to be able to respond to any incidents resulting from the audit.

2. Definitions

2.1 Refer Information Security Definitions document

3. Related Documents

3.1 Polices

(a) Information Security Policy

About this Document

Further information

TRIM Number	
Approval Authority	Chief Information Officer
Subject Matter Expert	Patrick McElhinney – Senior Security Specialist, IT Services
Contact Details	It-security@newcastle.edu.au
Review Date	1st July 2018

Approval History

No.	Effective Date	Approved by	Amendment
V1.0	31st March 2017	CIO	

---

[i] Red Hat Issue Severity Classification - https://access.redhat.com/security/updates/classification
[ii] Microsoft Severity Ratings - https://technet.microsoft.com/en-us/security/gg309177.aspx
[iii] Adobe Severity Ratings - https://helpx.adobe.com/security/severity-ratings.html
[iv] CVSS Scoring - https://nvd.nist.gov/cvss.cfm