Information Security Operations Management Manual

Section 1 - Audience

(1) All University staff, students, affiliates, vendors, volunteers, in all campuses and locations of the University, and at all times while engaged in University business or otherwise representing the University.

Section 2 - Executive Summary

(2) 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.

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

(4) 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.

Section 3 - Operational Procedures and Responsibilities

Objective – To ensure correct and secure operations of information systems

Documented Operating Procedures

(5) Information Owners, System Owners and System Administrators must ensure that Standard Operating Procedures (SOP):

a. are documented;
b. are approved by an appropriate authority;
c. are up to date and maintained;
d. are consistent with University policies, procedures, manuals and guidelines;
e. include a 'current as at [date]' or equivalent statement; and
f. are reviewed and updated:
    i. when there are changes to the solution architecture;
    ii. when there are changes in business processes or to system operations; or
    iii. following a related security incident investigation.

(6) SOPs for each system should cover the following:

a. high-level solution architecture design, including key integrations with other systems;
b. system administration and maintenance activities, such as managing backups and user accounts;

c. software and hardware configuration;
d. patch, update and upgrade processes;
e. log data management;
f. Disaster Recovery;
g. Business Continuity Plan; and
h. contact information for technical and business personnel.

Change Management

(7) Changes to business processes and information systems that effect information security must be controlled.

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

(9) The change management process must follow the guidelines, approvals and templates provided as per the University's Change and Release Management Process Manual.

(10) 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 for 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. confirming that planned change(s) were implemented as intended.

(11) System Owners must plan for changes by:

a. assessing the potential impact of the proposed change on security by conducting a security review or risk assessment;
b. identifying any impact on agreements, including information sharing agreements and licensing;
c. notifying affected internal and external parties;
d. obtaining approvals from relevant Information Owners; and
e. training technical and operational staff as necessary.

(12) System Administrators must implement changes by:

a. preparing change implementation plans that include testing and contingency plans in the event of problems;
b. following the documented implementation plans; and
c. confirming that the changes have been performed and no unintended changes took place.

Capacity Management

(13) The use of information system resources must be monitored and optimised with projections made to plan for future capacity requirements.

(14) System Owners and System Administrators are responsible for implementing capacity management processes by:

a. documenting current capacity requirements;

b. documenting capacity planning processes;
c. including capacity requirements in service agreements; and
d. monitoring and optimising information systems to detect impending capacity limitations.

(15) System Owners and System Administrators must project future capacity requirements based on:

a. statistical or historical capacity requirements;
b. projected business and information systems requirements; and
c. expected trends in information processing capabilities (e.g. introduction of more efficient hardware or software).

(16) System Owners and System Administrators must use trend information from the capacity management process, to identify and remediate potential bottlenecks that present a threat to system security or services.

Separation of Development, Testing and Production Environments

(17) Development and testing environments must be separated from production environments to reduce the risk of unauthorised access or accidental damage their integrity or contents.

(18) System Owners and System Administrators 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 specific authorised personnel;
e. prevent access to compilers, editors and other development and testing 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 Highly Restricted information in development, test or training systems.

Section 4 - Protection from Malware

Objective – To ensure that information systems are protected against malware.

Controls Against Malicious Code

(19) Detection, prevention and recovery controls, supported by user awareness activities, must be implemented to protect against malware.

(20) System Owners and System Administrators must protect University information systems from malicious code by:

a. installing, updating and using software designed to scan, detect, isolate and delete malicious code, configured with:
    i. signature-based detection enabled;
    ii. heuristic-based detection enabled;
    iii. detection signatures checked for currency and updated on at least a daily basis; and
    iv. automatic and regular scanning configured for all fixed disks and removable media;

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. refraining from reading emails, browsing the web, or obtaining files via online services, when authenticated with root or administrator privileges;
f. maintaining business continuity plans, that align to the University's Business Continuity Management Policy, to recover from malicious code incidents; and
g. maintain a critical incident management plan to identify and respond to malicious code incidents.

(21) University IT Security staff are responsible for communicating technical advice and providing information and awareness activities regarding malicious code.

Section 5 - Backup

Objective – To protect against loss of data

Information Backup

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

(23) Information Owners and System Owners must agree on, define and document backup and recovery processes, that consider the confidentiality, integrity and availability requirements of information and information systems.

(24) Backup and recovery processes must comply with:

a. the University Business Continuity Management Policy;
b. legislative, regulatory, University policy, and other obligations; and
c. records management requirements (refer Records and Information Management Policy).

(25) 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. physical and logical backup media management;
d. methods for performing, validating and labeling backups; and
e. methods for validating the recovery of information and information systems.

(26) Backup media and facilities must be appropriately secure based on a security review or risk assessment. Controls to be applied include:

a. use of 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 site.

(27) The backup frequency of information, software and configuration settings should be a function of business continuity requirements.

(28) Backups must be stored for three months or greater, depending on legislative and business requirements.

(29) Full backup and restoration processes must be tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

(30) Partial backup and restoration processes should be tested on at least an annual basis.

Section 6 - Logging and Monitoring

Objective – To log events and monitor compliance.

Event Logging

(31) System Owners must ensure that event logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed.

(32) 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.

(33) A centralised logging facility should be implemented, and systems configured to save event logs to the centralised logging facility as soon as possible after each event occurs.

(34) Where applicable, sufficient detail must be recorded in order for the event log to be useful, including:

a. date and times of the event;
b. the relevant user or process;
c. the event description; and
d. the ICT resources involved.

(35) For any system requiring authentication, logon, failed logon and logoff events must be logged.

(36) If event logging is disabled the decision must be documented and approved by the System Owner(s) of the affected system(s). This must include the name and position of the approver, date and rationale for de-activating the log. Systems must also log the event of disabling system logging itself.

(37) Event logs may be configured to alert someone if certain events or signatures are detected. 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 effected 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.

Protection of Log Information

(38) Information system logging facilities and log information must be protected against unauthorised access, modification and deletion.

(39) System Administrators must implement controls to protect logging facilities and log files from unauthorised modification, access or destruction. Controls must include:

a. physical security safeguards;
b. preventing administrators and operators from being able to modify, erase or de-activate logs; and
c. automatic archiving of logs to remain within storage capacity (capacity management).

Retention of Log Information

(40) Event logs can contribute to investigations following cyber security incidents, and should be retained for at least the life of a system. However, the retention requirement for these records under NSW State Archive's General Retention and Disposal Authority: Administrative Records (GA28) recommends that audit data should be retained for the period of the base transaction record, e.g. seven (7) years for financial system log data.

(41) System logs for systems that support the University's critical business processes must be retained for at least 30 days online and archived thereafter.

(42) Data centre physical access logs must be retained for at least seven (7) years.

(43) Logs must be retained indefinitely if an investigation has commenced, or it is known that evidence may be obtained from them, and until the investigation has concluded.

(44) Contact Records Governance Services (RGS) for further guidance on retention requirements for specific business information.

Administrator and Operator Logs

(45) Activities of privileged users must be logged and the log subject to regular review.

(46) The activities of System Administrators, operators and other privileged user(s) must be logged including:

a. the time an event (e.g. success or failure) occurred;
b. event details including files access, 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.

(47) Logs of the activities of privileged users should 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.

Operating System Logs

(48) The following events should be logged for operating systems:

a. transfer of data to external media;
b. system startup and shutdown;
c. service failures and restarts;
d. failed attempts to access data and system resources;
e. changes to system configurations;
f. changes to security policy;
g. changes to accounts;

h. attempts to use special privileges;
i. application crashes and any error messages; and
j. access to restricted or highly-restricted data and processes.

Web Application Logs

(49) The following events should be logged for web applications:

a. search queries initiated by users;
b. crashes and any error messages;
c. attempted access that is denied; and
d. login and logoff events.

Database Logs

(50) The following events should be logged for databases:

a. use of executable commands;
b. modifications to data;
c. database logons and logoffs;
d. database administrator actions;
e. changes to user roles or database permissions;
f. changes to the database structure;
g. database access attempts, whether successful or unsuccessful;
h. attempts to elevate privileges;
i. any query or database alerts or failures;
j. any query containing multiple embedded queries;
k. any query containing comments;
l. addition of new users, including privileged users; and
m. access to restricted or highly-restricted information.

Clock Synchronisation

(51) An accurate time source must be established and used consistently across systems and network devices to assist with the correlation of events.

(52) System Administrators must synchronise information system clocks to the local router gateway or a University-approved NTP service.

(53) System Administrators must confirm system clock synchronisation following power outages and as part of incident analysis and event log review.

Section 7 - Control of Operational Software

Objective – To ensure the integrity of production systems.

Installation of Software on Production Systems

(54) The installation of software on production information systems must be controlled.

(55) System Owners should ensure that their software libraries are adequately protected to prevent the corruption of information systems or the disruption of business operations.

(56) Access to operating system and operational or production application software libraries must be restricted to authorised staff only.

(57) To minimise the risk of damage to production systems, System Owners and System Administrators must implement the following procedures when installing software;

a. the updating of the operational software, applications and program libraries must only be performed by trained administrators upon appropriate authorisation;
b. production systems must not contain development code or compilers;
c. applications and operating system software updates must only be implemented after successful testing; the tests should cover usability, security, effects from and on other systems and user experience;
d. a configuration control system should be used to keep control of all implemented software as well as the system documentation;
e. a rollback strategy should be in place and previous versions of application software retained; and
f. old software versions should be archived with configuration details and system documentation.

(58) Vendor-supplied software used anywhere within the University ICT environment must be maintained at a level supported by the vendor.

(59) Physical or logical access to University systems should only be given to suppliers for support purposes when necessary and with the approval of the relevant System Owner.

Section 8 - Technical Vulnerability Management

Objective – To prevent exploitation of technical vulnerabilities.

Management of Technical Vulnerabilities

(60) Vulnerability assessments and penetration tests should be conducted by the University's Information Security Team before a system is deployed, after a significant change to a system, and at least annually or as specified by the system owner.

(61) To support technical vulnerability management, the Chief Information Officer (CIO) must maintain an inventory of ICT assets. 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.

(62) Vulnerabilities which impact University information systems must be addressed in a timely manner to mitigate or minimise the impact on University operations.

(63) Vulnerability remediation efforts, including patch implementations, shall be coordinated and processed according to the University's Information Security Patch Management Manual and prioritised based on the level of risk that the vulnerability introduces, according to the University's Risk Management Framework.

(64) Vulnerability assessments must be conducted both internal and external to the University ICT environment:

a. Internal Vulnerability Assessments:
    i. servers infrastructure;
    ii. desktops and workstations; and
    iii. network infrastructure;
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; and
    iv. cloud based services;

Vulnerability Management Cycle

Asset Discovery

(65) The IT DevOps team will share the IP segments of all University server and ICT infrastructure assets, including data centres and other Virtual LAN’s with the Information Security Team.

(66) The Information Security Team will perform an asset discovery scan for servers and ICT infrastructure on the network segments on a weekly basis.

(67) The list of identified assets will be scanned for vulnerabilities.

Scan – Remediate – Rescan

(68) The Information Security Team shall perform vulnerability analysis scans on all in-scope assets on a weekly basis.

(69) The Information Security Team will use the industry standard Common Vulnerability Scoring System (CVSS) to assess the inherent risk associated with identified vulnerabilities.

(70) The Information Security Team shall inform the System Owner or System Administrator regarding the results of the scans and share the vulnerability data for each system.

(71) All vulnerabilities identified in the VA Scan shall be remediated in accordance with the Remediation Timeline and Risk Acceptance (below).

(72) The System Owner or System Administrator shall inform the Information Security Team regarding the completion of vulnerability remediation.

(73) Vulnerabilities that cannot be actioned within the defined timeframe will need to be managed according to the requirements of the University's Risk Management Framework.

Ad-Hoc Scans

(74) Ad-hoc scans include scans on any new servers and services prior to production deployment as per the following process:

a. the System Owner or System Administrator shall create a new service request and submit to the Information Security Team for actioning;
b. the Information Security Team shall perform Vulnerability Analysis Scan of all systems and services related to the specified implementation;
c. the vulnerability assessment report shall be submitted to the implementation team;
d. the Information Security Team lead will validate with respective System Owners or System Administrator on

closure of the vulnerabilities, and then perform a re-scan;

e. vulnerabilities that cannot be actioned within the defined timeframe will need to be managed according to the requirements of the University's Risk Management Framework; and

f. assets / services / devices can be released to production only after the final sign off by Information Security Team, and the appropriate Change Management approval.

Classification of Vulnerabilities

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

Rating	Red Hat, Microsoft and Adobe Rating (see below)	Typical CVSS Score	Description
Critical	Critical	10	A vulnerability whose exploitation could allow malicious 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 of 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.

See: Understanding Red Hat Security Ratings; Microsoft Security Update Severity Rating System; Adobe Priority and Severity Rating Systems For Security Bulletins, and National Vulnerability Database Vulnerability Metrics (CVSS).

Remediation Timeline and Risk Acceptance

(76) All vulnerabilities identified in a Vulnerability Assessment Scan shall be addressed within the timeline described below.

(77) 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.

(78) Remediation time and risk acceptance for the identified vulnerabilities shall be as follows:

Vulnerability Level	Remediation Timelines		
	External Facing Devices	Internal Devices	Risk Acceptance
Critical	48 Hours	7 days	CIO, or System Owner, or Information Owner. (Dependent on delegation authority and Risk Management Framework management actions)

Vulnerability Level	Remediation Timelines		
	External Facing Devices	Internal Devices	Risk Acceptance
High	14 days	30 days	Associate Director, or System Owner, or Information Owner. (Dependent on delegation authority and Risk Management Framework management actions)
Medium	3 weeks	Next maintenance window	System Owner, or Information Owner.
Low	Next Maintenance window	Next maintenance window	System Owner, or Information Owner.

Third Party Scans

(79) A third party must be engaged annually to perform vulnerability assessment and penetration testing covering all internet facing University ICT services and systems.

Vulnerability Management Roles and Responsibilities

(80) The Information Security Team is responsible for:

a. performing regular asset discovery and vulnerability assessments;
b. overseeing vulnerability remediation;
c. targeting vulnerability program maturity through metrics development; and
d. monitoring security sources for vulnerability announcements and emerging threats that are relevant to the University's ICT resources.

(81) The System Owner is responsible for:

a. the IT asset that is scanned by the vulnerability management process. This role should decide whether identified vulnerabilities are mitigated or their associated risks are accepted; and
b. ensuring that System Administrators are charged with the effective management of their system.

(82) The System Administrator, is responsible for:

a. testing and evaluating options to mitigate or minimise the impact of vulnerabilities;
b. applying corrective measures to address the detected vulnerabilities; and
c. reporting to the System Owner and Information Security Team on progress in responding to vulnerabilities.

(83) Depending on how urgently a technical vulnerability needs to be addressed, the actions taken should be carried out according to the Change Management process, or by following the Information Security Incident Management Guidelines. For a high-risk technical vulnerability with wide-spread impact to the University (either being actively exploited or having the imminent potential to be exploited), the University Information Security Team will liaise with the University IT Management Team to assess the on-going risk to operations, options to mitigate the risk (i.e., patching vulnerable systems, disabling/turning off a service, implementing a border filter), and to establish expected remediation timelines. The University IT Management Team, led by the CIO, will make the final decision regarding the course of action.

(84) Responsibilities for vulnerability response must be included in service agreements with suppliers.

Restrictions on Software Installation

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

(85) Users are not allowed to install software on University devices unless specifically authorised by the relevant System Owner or System Administrator.

(86) System Administrators are responsible for the installation of software, updates and patches.

Section 9 - Information Security Audit Considerations

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

Information systems Audit Controls

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

(88) Prior to commencing compliance checking activities such as audits or security reviews of production systems, the CIO (or their delegate) 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 outside of agreed change blackout windows; and
h. appropriate personnel must be notified in advance in order to be able to respond to any incidents resulting from the audit.

Status and Details

Status	Historic
Effective Date	18th June 2019
Review Date	18th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	17th January 2023
Responsible Executive	Anthony Molinia Chief Digital & Information Officer +61 49138713
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Risk assessment" - The overall process of risk identification, risk analysis, and risk evaluation.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"ICT resources" - All information and communication technology resources and facilities.

"Information Owner" - A senior business, college or unit manager whom the University has authorised to collect, create, retain and maintain information within their assigned area of control.

"Personnel" - In relation to a party, any employee, officer, agent, contractor, sub-contractor, student or volunteer of that party.

"Program" - When referring to learning, a program is a sequence of approved learning, usually leading to an Award. For all other uses of this term, the generic definition applies.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.

"Third party" - A person or group other than the University or any of the University's partner institutions.

"University business" - Work that the University has directed to be undertaken which is required, essential, and beneficial for the functions of the University. This includes, but is not limited to, attending meetings, conferences or fieldwork, but does not include activity that is not location specific, e.g. email management, writing papers. University business may be undertaken by staff and non-staff.