# Patch and Vulnerability Management Framework

# Section 1 - Overview and Scope

(1) This Framework establishes an integrated patching and vulnerability management program covering the University, UNE's Controlled Entities, Research Centres and Institutes, and delegates.

(2) The Framework supports good judgment to be practiced in tailoring the implementation of this Framework's requirements to fit all UNE systems.  Where the Framework mandates a specific practice to be adhered to, this is clearly stated.

(3) All UNE hardware and software on the network are included in the patch and vulnerability management program.

(4) This Framework applies to Controlled Entities, Research Centres and Institutes, and delegates within or contracted by UNE and to the management of patching and vulnerabilities of all Information and Communications Technologies (ICT) infrastructure that is part of UNE's digital presence including but not limited to:

a. servers;
b. desktops and laptops;
c. applications; and
d. network devices.

(5) The following hardware and software are excluded from this Framework:

a. personal devices;
b. major upgrades (eg upgrading Windows 7 to Windows 10);
c. hardware upgrades; and
d. non-security related patches (eg new feature releases).

# Section 2 - Patch and Vulnerability Management Principles

### Principle 1 – All UNE representatives, delegates, research centres and institutes, controlled entities are required to know ICT infrastructure environment

### Principle 2 – The University will adopt a risk-based approach to patching and vulnerability management

(6) Where the risk owner decides not to patch the vulnerability then compensating controls are required to mitigate the risk.

### Principle 3 – Patch deployment should be automated wherever possible

(7) Automation of patch deployment is compulsory, unless otherwise authorised by the Chief Information Officer (CIO).

### Principle 4 – The University will continuously measure, improve and report patch compliance efforts using metrics

# Section 3 - Accountabilities and Responsibilities

(8) Patching and vulnerabilities will be managed in accordance with this Patch and Vulnerability Management RACI Table 1.

**Table 1: Patch and Vulnerability Management RACI**

| Activity | Responsible | Accountable | Consulted | Informed |
|---|---|---|---|---|
| Framework Ownership and Implementation | Security Governance Risk and Compliance Manager, Controlled Entities and Research Institutes Delegates | CISO, Deputy CISO, Heads of Controlled Entities and Research Institutes | IT Management Team | CIO |
| Review of Metrics | Security Governance Risk and Compliance Manager, Controlled Entities and Research Institutes Delegates | CISO, Deputy CISO, Heads of Controlled Entities and Research Institutes | IT Management Team, Security Operations Manager | CIO |
| Compliance Management | Security Governance Risk and Compliance Manager, Controlled Entities and Research Institutes Delegates | CISO, Deputy CISO, Heads of Controlled Entities and Research Institutes | IT Management Team | CIO |
| External Compliance Audits | Security Governance Risk and Compliance Manager, Controlled Entities and Research Institutes Delegates | CISO, Deputy CISO, Heads of Controlled Entities and Research Institutes | IT Management Team, Internal Audit | CIO |
| Asset Inventory and Management (including assets not managed by UNE) | Deputy CIO, Controlled Entities and Research Institutes Delegates | CIO, Directors and Heads of Controlled Entities and Research Institutes | Security Operations Manager, Security Governance, Risk and Compliance Manager | Deputy CISO, CISO and CIO |
| Vulnerability Scanning | Security Operations Manager, Third parties, Controlled Entities and Research Institutes Delegates | Associate Director Digital Operations, Directors, Heads of Controlled Entities and Research Institutes | TDS Teams, Security Governance, Risk and Compliance Manager | CIO, ITMT, Directors and Heads of Controlled Entities |
| ServiceNow ticket creation, management and monitoring | Security Operations Manager, Controlled Entities and Research Institutes Delegates | Associate Director Digital Operations, Directors, Heads of Controlled Entities and Research Institutes | TDS Teams, Security Governance, Risk and Compliance Manager | CIO and ITMT |
| Resolution of Vulnerabilities Identified through scanning activities | Deputy CIO, Associate Directors, Controlled Entities and Research Institutes Delegates | CIO, Directors and Heads of Controlled Entities and Research Institutes | Security Operations Manager, Security Governance, Risk and Compliance Manager | CIO and ITMT |

| Activity | Responsible | Accountable | Consulted | Informed |
|---|---|---|---|---|
| Vendor Notifications (subscribing to advisories eg AusCERT) | Deputy CIO, Associate Directors, Controlled Entities and Research Institutes Delegates | CIO, Directors, Heads of Controlled Entities and Research Institutes | UNE Governance, Security Operations Manager, Security Governance, Risk and Compliance Manager | Deputy CISO, CISO |
| Risk Management, testing, deployment and issue resolution of updates and patches | Deputy CIO, Associate Directors, Controlled Entities and Research Institute Delegates | CIO, Directors, Heads of Controlled Entities and Research Institutes | Security Operations Manager, Security Governance, Risk and Compliance Manager | CISO and Deputy CISO |
| Assist with the support risk assessments | Associate Director Digital Operations, Controlled Entities and Research Institutes Delegates | CIO, Directors and Heads of Controlled Entities and Research Institutes | UNE Governance, Security Operations Manager, Security Governance, Risk and Compliance Manager | Deputy CISO, CISO and CIO |
| Contracts include risk reduction clauses and compliance with the Patch and Vulnerability Management Framework as required | Associate Director Digital Operations, Controlled Entities and Research Institutes Delegates | CIO, Directors and Heads of Controlled Entities and Research Institutes | Security Operations Manager, Security Governance, Risk and Compliance Manager, Legal Services, Strategic Procurement | Deputy CISO, CISO and CIO |

## Patch and Vulnerability Management Lifecycle Requirements

### ICT Asset Inventory Ownership

(9) The Deputy CIO, TDS Associate Directors, Directors and Heads of Controlled Entities, Research Centres and Institutes must ensure that an up-to-date ICT asset inventory is maintained.

### ICT Asset Inventory Management Strategy

(10) A documented process for creating and managing an ICT asset inventory must be available and communicated to all team members by the asset owners.  The two suggested methods of ICT asset inventory management found in Table 2 could be used to document the ICT asset register.

**Table 2: ICT asset inventory management methods**

| Asset Inventory Type | Description | Requirement |
|---|---|---|
| Dynamic | ICT Asset Register created on the fly, by using a management application or a script to query assets on the network and return relevant information | The process or script required to query the relevant assets on the network must be document and made known to all team members. |
| Static | ICT Asset Register is created in collaboration software program which is static and must be updated manually | Teams using ICT asset register must include updates to the asset register as part of their change management process, ie prior to a change being marked as completed, the asset register must be updated.  Regular audits are required to provide assurance and accuracy. |

### Asset Inventory Accessibility

(11) An up-to-date ICT inventory must be made available by the Associate Director Digital Operations to the Security Governance, Risk and Compliance Manager to review and perform compliance checks, and to the Security Operations

Manager for scanning and incident response activities.

(12) ICT asset inventories must be stored in the electronic Records Management System (RMS) in accordance with the Records Management Rule and updated monthly or earlier if a significant change has occurred (eg roll out of a new network/infrastructure, the addition of network segments).

**Asset Inventory Details**

(13) ICT asset inventories must capture sufficient details to support the requirements detailed in this Framework. Table 3 provides an example of the details that should be captured against each asset class in the inventory:

**Table 3: Details to be captured against asset class**

| Assets | Example Details |
|---|---|
| Windows desktops and laptops<br>Apple Macintosh desktops<br>Unix and Linux servers<br>Network devices | Asset name<br>IP address<br>MAC addresses<br>Service tag/serial<br>Asset type<br>Vendor<br>Platform<br>OS type<br>OS version/patch version<br>Confidentiality/Integrity/Availability requirements<br>Technology/Business owner |
| Applications and Databases | Name<br>Version<br>Vendor<br>Service provider<br>Technology stack<br>Criticality<br>Business owner<br>Technology owner<br>Dependencies |

**Patch Identification**

(14) Depending upon the ownership of the system either by UNE, controlled entities, research centres and institutes, there must be a coordinated approach in place to facilitate the consistent and prompt identification of available patches. This is the initial step in ensuring that patches are evaluated and where appropriate, deployed within the environment. The asset owners will use both active and passive methods for the identification of patches through receiving vendor notification, reviewing patch bulletins and conducting active vulnerability scanning.

**Vendor Notifications**

(15) Responsible parties as outlined in the RACI Table 1 must define a method of receiving vendor notifications regarding newly available patches for each type of asset. This is generally achieved by actively monitoring or subscribing to advisories released by vendors or other groups such as AusCERT.

**Reviewing Patch Bulletins**

(16) Responsible parties as outlined in the RACI Table 1 must review each patch bulletin for the following security specific criteria prior to deciding whether to deploy the patches within the environment and timeframe for deployment:

a. list of all assets and versions affected;
b. technical details of the vulnerability including an overview of how exploitation occurs;
c. typical consequence of exploitation: code execution, information disclosure, denial of service etc
d. current exploitation status: whether the vulnerability is being publicly exploited;
e. the existence and details of any temporary workarounds; and
f. an overall measure of severity, based on the above factors.

(17) Non-security related patches will be reviewed on a business needs basis by the asset owners.

**Allocate Patch Risk Rating**

(18) Responsible parties must use the matrix found in Table 4 to evaluate and allocate a risk rating to patches prior to deployment. The risk rating will align with the patch installation timeframes defined within this Framework.

**Table 4: Risk matrix for evaluation and allocation of risk rating to patches prior to deployment**

| | **Consequence** | | | | | |
|---|---|---|---|---|---|---|
| **Likelihood** | | Insignificant | Minor | Moderate | Major | Severe |
| | Probable | Low | Medium | High | Extreme | Extreme |
| | Likely | Low | Medium | High | High | Extreme |
| | Possible | Very Low | Low | Medium | High | High |
| | Unlikely | Very Low | Low | Medium | Medium | High |
| | Rare | Very Low | Low | Low | Medium | Medium |

**Utilise a Risk-Based Approach for Critical or Time Sensitive Patches**

(19) A risk assessment must be constructed by the digital operations team or the team who owns the system or application being patched to establish the risk associated with the patches where patches cannot be tested thoroughly prior to deployment. The risk assessment outcome must be used to decide whether the risk to deploy patches without sufficient testing outweighs the risk associated with the vulnerability. Depending upon the system ownership the final risk acceptances is provided by the CIO or Directors and Heads of Controlled Entities, Research Centres and Institutes.

(20) Vulnerability likelihood ratings are defined in Table 5.

**Table 5: Vulnerability likelihood ratings**

| **Rating** | **Definition** |
|---|---|
| Probable | In the current contextual environment, exploitation of the vulnerability is expected to occur multiple times within a 12 month period, OR more than 80% of the time. |
| Likely | In the current contextual environment, exploitation of the vulnerability is expected to occur once within a 12 month period, OR 61%-80% of the time. |
| Possible | In the current contextual environment, exploitation of the vulnerability is expected to occur within a 5 year period, OR 31%-60% of the time. |
| Unlikely | In the current contextual environment, exploitation of the vulnerability is expected to occur within a 10 year period, or 5%-30% of the time. |

| Rating | Definition |
|---|---|
| Rare | In the current contextual environment, the corporate risk will only occur in exceptional or unforeseen circumstances. |

(21) Vulnerability impact ratings are defined in Table 6.

**Table 6: Vulnerability impact ratings**

| Rating | Definition |
|---|---|
| Severe | Community unable to function without significant support.<br>Key technologies no longer available, and no viable alternative exists.<br>Potential for major injury or fatalities.<br>Irreparable damage to relationships with key stakeholders and potential for UNE to cease operating in current form. |
| Major | Noticeable impact on user community.<br>Some core services unavailable.<br>Potential for serious distress or minor injury.<br>Sustained criticism from the majority of key stakeholders on the sustainability of UNE in its current form. |
| Moderate | Some inconvenience to the user community.<br>The ability to provide a service is severely compromised.<br>Moderate effort required to implement an alternative solution.<br>Public criticism from key stakeholders regarding the organisation’s services or activities. |
| Minor | Minor disruption to the user community.<br>The ability to provide the required service is impaired.<br>Complaints from key stakeholder requiring management attention. |
| Insignificant | Little disruption to the user community.<br>Technologies in use will require little/no effort to change.<br>An isolated complaint from an individual stakeholder is able to be managed via business as usual operations. |

### Patch Evaluation and Testing

(22) Patches that have been reviewed by ICT asset owner must be evaluated and tested prior to deployment. Patch evaluation must include allocating a risk rating to the patch to determine the timeframe in which the patch should be implemented. Depending on the risk rating and specified deployment timeframe, it may be necessary to conduct a reduced form of patch testing.

### Patch Testing Strategies

(23) Appropriate patch testing strategies must be developed, documented, and approved when testing patches. These strategies should include the testing principles found in Table 7 and consultation with business owners who are the key stakeholders of any asset where the patch will be applied against. The testing strategies should consider the context and risks of the environment to which the patches are being deployed. Testing must also take into consideration patch deployment timeframes.

**Table 7: Testing Principles**

| Asset Type | Principles |
|---|---|
| Computer lab devices | Test patches across a few selected devices in each computer room across each campus.<br>Computer labs in UNE run a varying selection of applications with unique application dependencies and requirements.<br>Patches may work in one lab but may prevent a class being conducted in another.<br>Awareness should be provided to lecturers and tutors that they should encourage the use of these patch testing devices and report any malfunctioning computers or applications promptly for review by client services. |
| Windows devices<br>Apple Macintosh | Patches should be tested on client services test devices first, prior to deployment to the remaining user base. |
| Windows servers<br>Unix and Linux servers<br>Applications<br>Databases | Initially, patches should be deployed and tested on a development or test environment.<br>Where only production environment exists, snapshots/backups should be taken prior to deployment of patches.<br>Business stakeholders should conduct necessary testing in non-production environments and provide formal approval to deploy patches in production environments. |
| Network devices | Patches should initially be deployed and tested on smaller or less critical network segments. |

**Patch Testing Exceptions**

(24) Depending upon the system for which excepting is being requested where the defined patch installation or testing timeframes cannot be met, it must be escalated to the CIO, Directors and Heads of Controlled Entities, Research Centres and Institutes by whom the system being exempted is owned.  the outcome of this may include delaying patch installation until testing can be completed, or testing may be fast-tracked where the likelihood and impact of compromise are unacceptable.  All respective stakeholders must be involved in a data and information security risk assessment to determine the best course of action.  Where testing cannot be fully completed, a modified deployment and testing strategy should be defined during the risk assessment to lessen the likelihood of any widespread outages.

**Patch Deployment**

(25) Patches must only be deployed once they have been fully tested and approved, or exempted by the CIO or Directors and Heads of Controlled Entities, Research Centres and Institutes.  Patches will generally be deployed during the monthly maintenance window unless they have been categorised as a critical or high-risk and approved by the CIO or Directors and Heads of Controlled Entities, Research Centres and Institutes.

**Formal Change Management Procedures**

(26) Patching for all production assets must be undertaken through their own formally defined Change Management Process.

**Patch Rollback and Contingency**

(27) Patch rollback planning must be undertaken prior to any approval of change management tickets.  Sufficient detail should be included in the patch and rollback plan, including how applications and data will be restored.  Where a third party is involved in patch deployment and the rollback procedure is being managed by them, UNE stakeholders must ensure the rollback procedure is captured in the UNE ServiceNow ticket.

**Patch Installation Timeframes**

(28) The patch installation timeframes found in Table 8 must be followed.

**Table 8: Patch installation timeframes**

| Patch Conditions | Patch Assessment Timeframe | Patch Completion Timeframe |
|---|---|---|
| Risk Rating is Critical<br>(or)<br>CVSS score of 9.0-10.0<br>(or)<br>Internet facing and an exploit exists | ASAP | 48 hours |
| Risk Rating is High<br>(or)<br>CVSS score 7.0-8.9<br>(or)<br>Internet facing | 3 days | 14 days |
| Risk Rating is Medium<br>(or)<br>CVSS score 4.0-6.9 | 15 days | 30 days |
| Risk Rating is Very Low – Low<br>(or)<br>CVSS score 0 – 3.9 | 30 days | 60 days |

**Patch Installation Timeframe Exceptions**

(29) If a patch cannot be installed within the Patch Completion Timeframe as mentioned in Table 8, this should be raised as a risk to the CIO, Directors and Heads of Controlled Entities, Research Centres and Institutes. A risk assessment must be completed to assess the risk and determine the controls that can be put in place to modify the risk of non-compliance. The non-compliance decisions must include a re-evaluation date, business owner, the Security Governance, Risk and Compliance team, and the Security Operations Manager must be notified of these decisions to track them in the Cyber Security Risk Register and for reporting purposes.

## Vulnerability Management

(30) A vulnerability scanning program must be defined and managed by the Security Operations Manager in accordance with RACI Table 1. The objective of the vulnerability management program is to provide a proactive approach in the identification of vulnerabilities which will be assigned to the relevant teams for remediation in line with this Framework. All UNE assets including hosted assets and associated and controlled entity assets are in scope, unless otherwise explicitly exempted by the CIO or Directors and Heads of Controlled Entities, Research Centres and Institutes.

(31) When deploying a vulnerability scanning solution, the considerations described in Table 9, should be reviewed.

**Table 9: Considerations when deploying a vulnerability scanning solution**

| Consideration | Description |
|---|---|
| Asset identification and prioritsation | Assets on the network should be identified using the asset registers maintained by respective teams.<br>Assets should be prioritised based on their criticality and risk exposure.<br>Asset groups should be created based on business value/risk, based on the asset's parameters.<br>Asset groups should be allowed to capture additional information relating to any systems and applications running on them. |
| Scanners should have sufficient network access | Scanners must be able to access assets which it intends to scan.<br>Where possible, authenticated scanning should be undertaken to provide the most accurate results.<br>Where possible, scanning should not be undertaken through a firewall. |

| Consideration | Description |
|---|---|
| Non-standard or legacy devices | Systems that can be considered non-standard or legacy should be reviewed closely prior to being included on a target list. |
| Vulnerability management process | A process should be developed and implemented to continually improve the identification and management of vulnerabilities. This would include:<br>Process for following up vulnerabilities that are not remediated within the defined timeframe (ie continue to appear on scan reports)<br>Process for identifying false positives and recording false positives to reduce security fatigue |
| Reporting | Scheduled vulnerability finding reports are produced and sent automatically to the Deputy CIO, Associate Directors, Directors, Controlled Entities, UNE Representatives, Research Centres and Institutes |

## Vulnerability Scanning

(32) The Security Operations team will be responsible for conducting vulnerability scanning of the UNE environment. Vulnerability scanning must be conducting on a continuous basis. When a vulnerability is identified, a ticket must be created in ServiceNow to track the vulnerability to resolution. Security Operations will notify the relevant team and liaise with the responsible party until resolution. The Deputy CIO, respective Associate Directors, Controlled Entities, Research Centres and Institutes delegates are responsible for addressing the vulnerability based on the patch risk rating and deploying within the timeframes specified in accordance with this framework.

## Vulnerability Reporting

(33) The Security Operations Manager will produce:

a. Weekly vulnerability reports on ICT assets grouped by risk rating. Any unremedied vulnerabilities breaching Patch Installation Timeframes must be identified in the reports for non-compliance tracking;
b. A vulnerability report on all ICT assets and report to Security Governance, Risk and Compliance Manager for review and action.

## Patch and Vulnerability Metrics

(34) Patch and vulnerability metrics support continuous improvement of UNE's patch and vulnerability management capability. Metrics are captured and reported to the Security Governance, Risk and Compliance Manager to provide management and operational teams with guidance on further improving UNE patch and vulnerability processes. The majority of these metrics are collected by the Security Operations Manager using a vulnerability scanner and a review of ServiceNow tickets. The metrics described in Table 10 are to be captured and reported at least quarterly.

**Table 10: Metrics to be captured and reported**

| Metric | Description |
|---|---|
| Patch timeframe non-compliance | Instances where the patch installation timeframes were unable to be met, over a given period. |
| Average time to patch | Average time to implement critical or high-risk patch by system after evaluation, over a given period. |
| Scanning coverage | Scanning scope metrics should be based on asset groups:<br>Number of machines included in scan<br>Number of machines not scanned<br>Number of missing patches |
| Critical patch coverage | Number of assets missing latest critical or high-rated patches, over a given period. |

| Metric | Description |
| --- | --- |
| Patch exceptions granted | Number of exceptions granted through the Information Security Risk Management Framework for missing patches. |

# Section 4 - Authority and Compliance

(35) The Vice-Chancellor and Chief Executive Officer (VC&CEO) makes this Policy pursuant to Section 29 of the University of New England Act 1993 (NSW).

(36) The Policy Steward, the Chief Information Officer, is authorised to make associated documents for the operation of this Policy, providing they are consistent with this Policy.

(37) UNE's Controlled Entities, Research Centres and Institutes, and delegates must observe this policy.

(38) The VC&CEO may approve an exception to this Policy where the VC&CEO determines the application of this Policy would otherwise lead to an unfair, unreasonable or absurd outcome.  Approval by the VC&CEO under this clause must:

a. be documented in writing;
b. state the reason for the exception; and
c. be registered in the approved UNE electronic Records Management System (RMS) in accordance with the Records Management Rule.

(39) This Framework operates from the Effective Date.

(40) Previous Frameworks associated with patch and vulnerability management are replaced and have no further operation from the Effective Date of this new Framework.

# Section 5 -  Definitions (specific to this Policy)

(41) Patch – means software and operating system (OS) updates that address security vulnerabilities within a program or product.

(42) Discovery – means exercise involving identifying the number of unpatched systems and relevant missing patches referencing the available patches to be applied.

(43) Vulnerability – means a flaw or weakness in an ICT asset, its security procedure, internal controls, or design and implementation, which could be exploited or triggered by a threat source.

## Status and Details

| | |
|---|---|
| **Status** | Not Yet Approved |
| **Effective Date** | To Be Advised |
| **Review Date** | To Be Advised |
| **Approval Authority** | Vice-Chancellor and Chief Executive Officer |
| **Approval Date** | 8th December 2023 |
| **Expiry Date** | To Be Advised |
| **Unit Head** | Angie Hendrick<br>Chief Information Officer<br>02 6773 2044 |
| **Author** | Angie Hendrick<br>Chief Information Officer<br>02 6773 2044 |
| **Enquiries Contact** | Angie Hendrick<br>Chief Information Officer<br>02 6773 2044<br><br>Technology and Digital Services<br>+61 2 6773 5000 |

## Glossary Terms and Definitions

**"Records Management System (RMS)"** - The University of New England installation of HP TRIM, or equivalent replacement system, under the control of the Records Management Office.