THE UNIVERSITY OF NOTRE DAME AUSTRALIA

# Information Technology Instruction:

# Vulnerability Management and Security Patching

Effective: 23 October 2023

Audience: Employees, Students

| | |
|---|---|
| Key words: | Patching, vulnerabilities, data, information, information security |
| Instruction Owner: | Chief Information Officer |
| Responsible Officer: | Director, IT Business Partners & Security |
| Review Date: | 23 October 2024 |

# Information Technology Instruction: Vulnerability Management and Security Patching

## 1. Authority and force of this instruction

The *Policy: Information and Information Technology* authorises the Chief Information Officer (CIO) to maintain detailed instructions for staff to ensure security of the University's information (clause 5.3.1.2).

The *Procedure: Information Management* authorises the CIO to maintain instructions for staff to ensure 'secure use of university-provided software, personal computers, mobile devices and tablet' (clause 12.4.1.2).

## 2. Instruction

*Scope*

2.1. This instruction applies to all staff who are business owners of, support or use university-provided information systems or software.

2.2. It does not apply to information systems, software or external data storage provided by a third party as a cloud computing service or software as a service: for requirements in relation to information security of such systems/software, see the IT Instruction: Cloud Computing and Software as a Service.

*Routine upgrade/patches schedule*

2.3. In consultation with business owners of university information systems, the Operations team of Information Technology will maintain a schedule of system upgrades and non-urgent patches, to minimise disruption to university business.

*Decisions to patch urgently*

2.4. However, the Director, IT Business Partners and Security may decide that:

- a security patch will be made urgently to a system or to university-provided software, to remove a vulnerability that poses a significant risk to business continuity or to privacy or security of university information, and
- when the patch will be made.

*Identifying and assessing vulnerabilities*

2.5. The Cybersecurity team of Information Technology is responsible for identifying vulnerabilities of systems and software, and assessing their level of risk.

2.6. Information Technology will at least annually engage a third-party information technology specialist to assess and penetration-test all internet-facing university information systems for vulnerabilities.

2.7. The risk of each vulnerability will be assessed by considering:

- the likelihood of adverse events that the vulnerability allows
- how severe the effects of the adverse events would be if they occurred, and
- how important the system or software is for business continuity and in terms of the classification level of the information it creates or holds.

*Rectifying vulnerabilities*

2.8. The Operations team of Information Technology is responsible for mitigating and rectifying vulnerabilities, for example by

- applying vendor-provided patches to remove the vulnerability, or
- for university-developed software, applying a fix or update to remove the vulnerability, or
- removing software from the system or from use altogether.

2.9. Where a vulnerability is assessed as of low or moderate risk, the Director, IT Business Partners and Security may decide that the system or software can be patched/upgraded to rectify the vulnerability at the time of the next scheduled upgrade/patch of the relevant system or software.

2.10. Where a vulnerability poses a high risk to security of sensitive university information or business continuity, the Director, IT Business Security will decide what action will be taken to rectify it, and how quickly, even where this involves temporary removal of access to the relevant system or reduction in functionality.

2.11. The director will consult the business owner of the relevant system to understand the effects of an unscheduled upgrade or patch.

2.12. In such cases, the vulnerability will:

- be logged as an IT incident so that work to resolve it is tracked, and
- if the vulnerability is already resulting in unauthorised access to sensitive university information or disruption to business, also be handled by the critical incident process: see the Procedure: Critical Incident Management.