THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Information Technology Instruction:

Software Information Security

Effective: 23 October 2023

Audience: Employees, Students

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

Information Technology Instruction: Software Information Security

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), and
- requires everyone who uses a university information system or a device provided by the University to follow those instructions (clause 5.1.3), and abide by the terms and conditions of use of the system or device.

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 tablets' (clause 12.4.1.2).

The *Procedure: Information Technology* (clause 8.2) authorises the CIO to 'maintain lists of what software staff can install on types of device provided by the University'.

2. Instruction

Scope

2.1. This instruction applies to all:

2.1.1. staff

2.1.2. software used on university networks, servers, computers and devices, and

2.1.3. computers and devices with which anyone accesses university information technology networks.

3. Control of software and of access to university networks

Information Technology:

3.1. will maintain a register of software applications used for university business

3.2. will periodically assess and review such software, including whether the number of users of the software is within the number of licences the University holds for the software

3.3. will scan university networks, servers and devices for unauthorised or out-of-date software that may pose an information security risk

3.4. may remove software from networks, servers and devices to maintain information security or where user numbers exceed licences

3.5. will scan users' own computers and mobile devices used to access university networks, to check whether they have up-to-date operating systems or include malware, and

3.6. may block a user's computer or mobile device from access to a university network where the access may pose a risk to information security.

Decisions to cease using software

3.7. Where software has been approved for use on university business in the past, the Chief Information Officer may decide that the software will no longer be used, or its use will be limited or segregated from university networks, on criteria such as that:

- the software is no longer supported by the supplier, and poses a risk to business continuity, and/or
- the software (whether supported or not) poses risks to security of the University's information.
- In making such decisions, and setting a deadline after which the software must no longer be used, the CIO will consult units using it to understand the effects on business of removing the software.