Title	**Describe risks and implement security solutions when using digital tools**		
Level	**3**	**Credits**	**5**

Purpose	People credited with this unit standard are able to: identify and describe risks and compliance requirements when using digital devices and digitally stored and transmitted information in an organisational context; and explain procedures and implement solutions to meet end user security and good practice requirements when using digital tools in an organisational context. This unit standard has been developed primarily for assessment within programmes leading to the qualification New Zealand Certificate in Computing (Intermediate User) (Level 3) [Ref: 2592].

Classification	Computing > Generic Computing

Available grade	Achieved

Guidance Information

1 Recommended skills and knowledge:
Unit 32975, *Use digital tools securely, safely, ethically and legally*, or demonstrate equivalent knowledge and skills.

2 Assessment, where applicable, will be conducted in and for the context of a real or realistic situation and/or setting, and be relevant to current and/or emerging practice. The assessor may gather evidence over time from a range of scenarios rather than using one assessment where the learner has to demonstrate all of the required skills.

3 The tasks must be of sufficient complexity to provide scope to meet the assessment performance criteria. The assessment context for this unit standard must be suitable to meet the criteria for level 3 in the NZQF Level Descriptors, which are available by searching for “level descriptors” at www.nzqa.govt.nz.

4 Definitions
Anti-malware is the generic term used to describe the prevention, detection, and removal of malicious software/code such as viruses, Trojans, worms, backdoor, spyware and other harmful programs.
Digital devices refer to electronic computing devices that can receive, store, process or send digital information, such as computers (desktop or laptop), tablets, smartphones or other emerging digital technologies.

Digital tools refer to both hardware (storage and display devices) and software (applications and programs).
Good practice refers to practices to protect and secure digital tools and information by users, including selecting and using the appropriate feature or function to enable the safe and correct use of the chosen digital devices and platforms.
Health and safety hazards refer to physical and mental discomfort, pain or injury; visual discomfort; stress; fatigue; potential injury or harm from furniture (e.g. desks and chairs); environment (e.g. light, noise, temperature and air quality); placement of digital device components (e.g. mouse, keyboard, screen).
Malware refers to a type of malicious software/code that includes viruses, Trojans, worms, backdoor, spyware and other harmful programs.
Organisation refers to the context the digital tools are being operated in (e.g. businesses, clubs, not-for-profit organisations). It does not define or limit the situations in which assessment evidence may be gathered.
Requirements mean the documented policies and procedures or commonly accepted practices of a workplace, school or training provider. The learner must be given access to the policy and procedures prior to being assessed against this unit standard.
Security risks refer to the transparency and accessibility of information and maintaining basic security requirements, to prevent and minimise harm, in a home, work or study context.
Security solutions refer to practices to protect and secure digital tools and information by users such as – log-off, shut-down, physical security, anti-malware software, browser settings, firewalls; access control, locking, passwords; back-up and restore techniques; frequency of saving; virus protection facility; Uninterrupted Power Supply (UPS) or surge protector; personal network protection; read only files.
Transparency refers to visibility and openness of information.

5 Legislation relevant to this unit standard may include but is not limited to the:
Copyright Act 1994
Copyright (New Technologies) Amendment Act 2008
Crimes Act 1961
Harmful Digital Communications Act 2015
Health and Safety at Work Act 2015
Privacy Act 2020
Unsolicited Electronic Messages Act 2007
and any subsequent amendments.
Current legislation and regulations can be accessed at http://legislation.govt.nz.

6 Reference
ACC5637 Guidelines for Using Computers - Preventing and managing discomfort, pain and injury. Accident Compensation Corporation - Department of Labour, 2010; available from WorkSafe New Zealand, at https://www.worksafe.govt.nz/topic-and-industry/work-related-health/ergonomics/safely-using-computers-at-work/.

Outcomes and performance criteria

Outcome 1

Identify and describe risks and compliance requirements when using digital devices and digitally stored and transmitted information in an organisational context.

Range compliance refers to legislation and regulations that include but are not limited to – privacy, health and safety, copyright, spamming, software licencing; may include internal policies such as access control, acceptable use policy.

Performance criteria

1.1 Legal and regulatory risks are identified and described in terms of their implications for data, systems and organisational processes.

Range includes but is not limited to – security risks, privacy risks, copyright.

1.2 Organisational compliance requirements are identified and described in terms of using digital tools, and the transmission and storage of data.

1.3 Potential health and safety hazards associated with the use of digital tools are identified and described in terms of personal health, wellbeing and prevention of harm.

Range minimum of five potential health and safety hazards.

Outcome 2

Explain procedures and implement solutions to meet end user security and good practice requirements when using digital tools in an organisational context.

Performance criteria

2.1 Procedures to address security and privacy risks and meet good practice requirements in an organisational context are explained in terms of their impact on end users when using digital tools.

Range common security and privacy risks include but are not limited to – data interception and unauthorised access; malware; natural disaster; data corruption; hardware failure; network access.

2.2 Security solutions to meet end user security requirements in an organisational context are adopted when using digital tools.

Range solutions include but are not limited to – maintaining security measures and updates; anti-malware solutions; demonstrating compliance with organisational procedures and good practice.

2.3 Procedures and solutions to address potential health and safety hazards associated with the use of digital tools are described and implemented in terms of personal health and wellbeing and prevention of harm.

Range includes safe work practices when using digital tools.

Planned review date	31 December 2026

Status information and last date for assessment for superseded versions

Process	Version	Date	Last Date for Assessment
Registration	1	19 January 2017	31 December 2024
Review	2	28 April 2022	N/A

Consent and Moderation Requirements (CMR) reference	0099

This CMR can be accessed at http://www.nzqa.govt.nz/framework/search/index.do.

Comments on this unit standard

Please contact Toi Mai Workforce Development Council qualifications@toimai.nz if you wish to suggest changes to the content of this unit standard.