ICT and Cyber Security Management Policy and Procedure

Approving body	Governing Board
Date approved	27 Feb 2025
Date of effect	Commencement of operation
Next scheduled review	Two years from policy commencement
Policy owner	Chief Executive Officer
Policy contact	Chief Executive Officer
Related Documents	Facilities and Resources Plan Business Continuity Plan Compliance Management Framework Student Use of ICT Policy and Procedure Library Services and Learning Resource Policy and Procedure Personal Information and Privacy Policy and Procedure Records and Data Management Policy and Procedure
Other Relevant Documents	Australian Cyber Security Centre Strategies to Mitigate Cyber Security Incidents Australian Cyber Security Information Security Manual (ISM) Australian Cyber Security Centre Cyber Security Principles
Higher Education Standards Framework (HESF) 2021 (Cth)	Standard 2.1.2-3 Standard 2.3.4 Section 3.3 Section 6.2i Standard 7.3.3

Purpose

1.   This policy provides **Zenith Innovation Institute** (**Zenith / the Institute**) with a framework of roles, responsibilities, and principles for the management of the Institute's ICT systems including cyber security, and an overview of its key ICT (systems.

Scope

2.   This Policy applies to:

(a)   all staff of at the Institute, whether full-time, part-time, casual or contract;

(b)   members of the Institute's governing bodies;

(c)   all students; and

(d)   all information technology tools and resources as outlined in the Definitions.

Policy

3.   Zenith is committed to maintaining information security by:

(a)   ensuring that information systems and records are maintained, securely and confidentially to prevent unauthorised or fraudulent access to private or sensitive information as outlined in the *Records and Data Management Policy and Procedure*;

(b)   promoting and fostering a safe environment, including advising students and staff on actions they can take to enhance safety and security online outlined in the *Student Wellbeing Policy and Procedure*, *Health and Safety Policy and Procedure* and *Student Use of ICT Policy and Procedure*;

(c)   planning for, responding to and managing critical incidents (including cyber security incidents) that may impact the Institute and its community, as outlined in the *Critical Incident and Emergency Management Policy and Procedure*;

(d)   taking preventative action to mitigate foreseeable risks to academic integrity outlined in the *Student Academic Integrity Policy and Procedure*; and

(e)   exercising due diligence to identify, prevent, and manage risks within the Institute as per the *Due Diligence Policy and Procedure*, *Risk Management Framework* and *Business Continuity Plan*.

4.   ICT systems support both the governance of the Institute and the day-to-day management of its operation. These systems enable critical business processes and, as such, must be adequately developed, secured, maintained, and improved. ICT system users must also be appropriately trained and supported to operate them properly and effectively including ensuring secure authorised access and use of these systems.

5.   Zenith's ICT systems are managed according to the following principles:

(a)   **Requirements**: The Institute will identify and prioritise requirements for ICT systems, which must satisfy the requirements outlined in the *Higher Education Standards Framework (Threshold Standards) 2021*, including quality, sufficiency, access, security, safety, and privacy;

(b)   **Selection**: Zenith will select ICT systems in accordance with transparent criteria, including prioritised requirements, budgetary constraints, student and/or staff feedback, and reputation;

(c)   **Maintenance**: The Institute will have adequate resources for the maintenance of ICT systems. Where maintenance is outsourced, an adequate service level agreement will be entered into with the supplier;

(d)   **Support**: Zenith will have adequate support for users of ICT systems. For each system, users will be inducted, trained, and receive support and advice when needed;

(e)   **Risk management**: The Institute will identify, assess, and treat risks for each ICT system. For each ICT system, a responsible officer is designated for coordinating risk management activities in accordance with the Institute's *Risk Management Framework* and *Risk Management Plan and Sample Register*; and

(f)   **Review and improvement**: The Institute will review the adequacy of ICT systems and associated arrangements every year or earlier in accordance with relevant contractual agreements). The responsible officer will coordinate the review and the implementation of improvements.

Zenith ICT Systems

Learning Management System

Name	Software Used
Description	LMS which has a proven track record of being able to deliver a sustainable and reliable platform for students. The LMS will be hosted on NeXus Business Technology located in Sydney.
Arrangement	Service Agreement
Support	Support and training services to staff include: • Face-to-Face training (both standard and customised); • Online webinars; • extensive user-guide library; • Service Desk with a ticket tracking system
Back-up	Daily
Security	Secure hosting
Responsible Officer	IT and Systems Manager with input from Student Services Manager.
Review	Annually or earlier as required.

Zenith Website

Description	The Institute's website is the primary channel for representing the Institute's education offerings, governance, policies and forms, practical information, and relevant contact details. The website also provides a link to the Student Portal and to the online Library.
Arrangement	Design and maintenance of the website is outsourced to web designer contractor.
Support	Support to navigate the website and the Student Portal will be provided by Student Services.
Back-up	Monthly.
Security	Secure hosting.
Responsible Officer	Marketing Manager
Review	Every 6 months.

Zenith Student Management System

Name	Software Used
Description	The Student Management System is the Institute's platform for managing student data across the whole student lifecycle from enrolment to graduation and supports key administrative processes such as scheduling, recording of marks and grades or the creation of academic transcripts. The Student Portal is a component of the Student Management System and provides each student with easy access to enrolment information, records of transactions with the Institute, and other personal information.

Name	Software Used
Arrangement	Subscription for provision of software and hosting of data.
Back-up	Monthly
Security	Securely hosted.
Responsible Officer	IT and Systems Manager with input from Student Services Manager.
Review	Annually or earlier as required.

Zenith Library/Learning Resources Management System

Name	Software Used
Description	The Institute's Library/Learning Resources Management System manages all transactions relating to acquisitions, cataloguing, and borrowing.
Arrangement	Web-based library management system.
Back-up	Real-time back-up.
Security	Secure certified T4 hosting, role-based access, password policy.
Responsible Officer	Learning Resources Coordinator and Student Learning Support Officer.
Review	Annually or earlier as required.

Zenith Professional Applications

Accounting

Description	The Institute's Accounting Information Software records and processes all transactions relating to accounts payable and receivable, maintains a general ledger, and generates financial reports for management.
Arrangement	Cloud-based accounting software.
Back-up	Real-time data replication between geographically diverse, protected facilities, to ensure data is available and safely stored.
Security	Securely hosted.
Responsible Officer	Chief Executive Officer (CEO)
Review	Annually or earlier as required.

Records Management

Name	Software Used
Description	The Institute's Records Management System is the repository for all statutory books and records, excluding student records which are maintained in the Student Management System.

Name	Software Used
Arrangement	Cloud Based Subscription.
Back-up	Weekly.
Security	Securely hosted.
Responsible Officer	Academic Registrar / Student Services Manager
Review	Annually or earlier as required.

ICT and Cyber Security Infrastructure

Networks

Description	Zenith has implemented protocols, tools, and strategies to protect their digital assets, including data, ICT systems, and networks, from various threats.
Arrangement	Subscription
Security	Firewall, antivirus, password policy, Intrusion Detection Systems (**IDS**) and Intrusion Prevention Systems (**IPS**).
Responsible Officer	IT and Systems Manager
Review	Every 6 months.

Servers

Description	Secure system to ensure records are accessible and stored securely in line with relevant legislation and guidelines.
Arrangement	Cloud Based Subscription.
Back-up	Daily
Security	The security of Google Drive is ensured through encryption in transit and at rest, along with robust access controls and multi-factor authentication
Responsible Officer	IT and Systems Manager
Review	Annually or earlier as required.

Access to ICT Systems

6. Where possible, the Institute will provide off-campus access to student ICT systems through the Institute's website.

7. On-campus facilities for learning and teaching purposes include:

   (a) Learning and teaching spaces.

   (b) Learning and teaching resources including library, research and on-line textbooks as relevant

8. Staff and students have access to:

   (a) Desktops, laptops, or tablets depending on the needs.

9. Professional staff have access to dedicated desktops, laptops, or tablets depending on business needs.

ICT and Cyber Security

10. The Institute implements a range of strategies, including monitoring and updating its *Risk Management Plan and Risk Register* which includes a *Risk Incident Register*, to ensure the security of its ICT systems. Controls to be implemented by Institute staff or required from students and third-party suppliers include:

    (a) awareness and training, such as:

       (i) induction for new employees and students;

       (ii) cyber security awareness activity tailored to specific users;

       (iii) Institute policies and expectations, e.g. *Student Use of ICT Policy and Procedure*;

       (iv) contractual obligations of employees, students, and third parties relating to the use of ICT systems; and

       (v) identity management and access control, such as:

          (A) access authorisation;

          (B) least privilege;

          (C) segregation of duties;

          (D) remote access permissions;

          (E) defined processes for the review, disabling, or removal of access;

          (F) physical access restrictions;

    (b) protective technologies, such as:

       (i) session timeout;

       (ii) event log details;

       (iii) restrictions on removable media;

       (iv) prioritisation of recovery of critical ICT systems; and

       (v) cloud security requirements, such as selection of reputable and adequate provider of cloud services;

    (c) data security measures, such as:

       (i) protection of data at-rest or in-transit via encryption;

       (ii) security standards for the Institute's network, e.g. firewalls and routers;

       (iii) network diagrams and review of configuration;

       (iv) development of systems and network capacity plans for ensuring continued access of systems to students and staff;

       (v) back-up strategy and definition of required scope, frequency, methodology, location, and testing of back-ups; and

       (vi) ICT systems and network change management, including change history, impact, and approval for changes;

    (d) detection of cyber events, such as:

       (i) identification of anomalies;

       (ii) intrusion management;

       (iii) malware detection;

(iv)   monitoring of personal activity; and

(v)   monitoring of external parties' use of the Institute's ICT systems.

11.   Students and staff are required to take active steps to prevent inadvertent breaches and to report any online incident, hazard, or near-miss to Institute staff.

12.   Data and incident reports on ICT security obtained through the Institute's channels (e.g. reports made under the *Student Use of ICT Policy and Procedure* or *Health and Safety Policy and Procedure*) will be shared with the responsible officer through the Executive Management Committee for corrective action and continuous improvement.

Responsibilities

Responsibility	Responsible for:
CEO	The CEO is responsible for overseeing the selection, purchase, maintenance, and improvement of ICT and Cyber Security systems as supported by the Executive Management Committee, and ensuring that an annual internal audit is conducted to assess system security, compliance, and effectiveness.
All staff	All staff are responsible for: • abiding by procedures, protocols and processes for the proper use of ICT systems; and • reporting any issue to the responsible officer or supplier as appropriate.
Responsible officers	Responsible officers are responsible for: • conducting risk management activities for designated ICT systems; and • conducting reviews of the adequacy of designated ICT systems.

Definitions

13.   For the purposes of this Policy:

Term	Definition
Information and Communications Technology (**ICT**)	Technological tools and resources used to transmit, store, create, share or exchange information which are provided by the Institute, including email accounts, student portal, learning management system, online library collection, access to the internet, and general and specialist software.
Cyber Security	Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.
Cyber Security Incident	An unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Version Control

Version	Changes	Approval Body	Approval Date
1.0	Original Version	Governing Board	

Version	Changes	Approval Body	Approval Date
1.1	All actual software names moved to a schedule 1 The policy does not specify any actual names as discussed and they are all listed in the Schedule 1	Governing Board	19 Sep 2024
1.2	Under Related Documents removed the external documents and created a new row called "Other Relevant Documents" Point 4 added "effectively including ensuring secure authorised access and use of these systems" Point 5 f) replaced "three years" with "every year" Under CEO responsibility added "and ensuring that an annual internal audit is conducted to assess system security, compliance, and effectiveness" Point 12 replaced "Senior Management Team" with "Executive Management Committee"		
1.3	Updated IT contact and LMS contractor	Governing Board	27 Feb 2025

Schedule 1

Zenith ICT Systems

Learning Management System

Name	Moodle
Description	Moodle LMS which has a proven track record of being able to deliver a sustainable and reliable platform for students. The LMS will be hosted on NeXus Business Technology located in Sydney.
Arrangement	Service Agreement
Supplier	Subscription for provision of software and hosting of data
IT Support	Registered users may contact NeXus for any service requests.
Support	Support and training services to staff include: • Face-to-Face training (both standard and customised); • Online webinars; • extensive user-guide library; • Service Desk with a ticket tracking system
Back-up	Daily
Security	Secure hosting
Responsible Officer	IT and Systems Manager with input from Student Services Manager.
Review	Annually or earlier as required.

Zenith Website

Description	The Institute's website is the primary channel for representing the Institute's education offerings, governance, policies and forms, practical information, and relevant contact details. The website also provides a link to the Student Portal and to the online Library.
Arrangement	Design and maintenance of the website is outsourced to web designer contractor.
Supplier	NeXus Business Technology
IT Support	Users may contact Student Services for any question on the website.
Support	Support to navigate the website and the Student Portal will be provided by Student Services.
Back-up	Monthly.
Security	Secure hosting.
Responsible Officer	Marketing Manager
Review	Every 6 months.

Zenith Student Management System

Name	MeshEd
Description	The Student Management System is the Institute's platform for managing student data across the whole student lifecycle from enrolment to graduation and supports key administrative processes such as scheduling, recording of marks and grades or the creation of academic transcripts. The Student Portal is a component of the Student Management System and provides each student with easy access to enrolment information, records of transactions with the Institute, and other personal information.
Arrangement	Subscription for provision of software and hosting of data.
Supplier	MeshED
Support	Support and training services to staff include: • Face-to-Face training (both standard and customised); • Online webinars; • extensive user-guide library; • Service Desk with a ticket tracking system; and • Client access portals.
Back-up	Monthly
Security	Securely hosted.
Responsible Officer	IT and Systems Manager with input from Student Services Manager.
Review	Annually or earlier as required.

Zenith Library/Learning Resources Management System

Name	Liberty
Description	The Institute's Library/Learning Resources Management System manages all transactions relating to acquisitions, cataloguing, and borrowing.
Arrangement	Web-based library management system.
Supplier	Softlink
Support	Support and training services to staff include: • Face-to-Face training (both standard and customised); • Online webinars; and • Service Desk with a ticket tracking system.
Back-up	Real-time back-up.
Security	Secure certified T4 hosting, role-based access, password policy.
Responsible Officer	Learning Resources Coordinator and Student Learning Support Officer.
Review	Annually or earlier as required.

Zenith Professional Applications

Accounting

Description	The Institute's Accounting Information Software records and processes all transactions relating to accounts payable and receivable, maintains a general ledger, and generates financial reports for management.
Arrangement	Cloud-based accounting software.
Supplier	MyoB
Support	Frequent product updates. Free and unlimited 24/7 online customer support.
Back-up	Real-time data replication between geographically diverse, protected facilities, to ensure data is available and safely stored.
Security	Securely hosted.
Responsible Officer	Chief Executive Officer (CEO)
Review	Annually or earlier as required.

Records Management

Name	Google Drive
Description	The Institute's Records Management System is the repository for all statutory books and records, excluding student records which are maintained in the Student Management System.
Arrangement	Google Workspace Subscription
Supplier	Google
Support	24/7 help desk support. Product update and online customer support.
Back-up	Weekly.
Security	Securely hosted.
Responsible Officer	Academic Registrar / Student Services Manager
Review	Annually or earlier as required.

ICT and Cyber Security Infrastructure

Networks

Description	Zenith has implemented protocols, tools, and strategies to protect their digital assets, including data, ICT systems, and networks, from various threats.
Arrangement	McAfee Subscription

Security	Firewall, antivirus, password policy, Intrusion Detection Systems (**IDS**) and Intrusion Prevention Systems (**IPS**).
Responsible Officer	IT and Systems Manager
Review	Every 6 months.

Servers

Description	Secure system to ensure records are accessible and stored securely in line with relevant legislation and guidelines.
Arrangement	Google Workspace Subscription
Back-up	Daily
Security	The security of Google Drive is ensured through encryption in transit and at rest, along with robust access controls and multi-factor authentication
Responsible Officer	IT and Systems Manager
Review	Annually or earlier as required.