POLICY C33.0

INFORMATION AND CYBER SECURITY

1.0 INTRODUCTION

1.1 Context

Scentia and its subsidiaries, the Australasian College of Health and Wellness Pty Ltd (ACHW), the Australian Institute of Management Education and Training Pty Ltd (AIM) operating as AIM Business School (ABS), and AIM VET, a Registered Training Organisation (RTO), collectively 'the Scentia Group' is committed to managing information as an organisational asset which is created, used and share effectively whilst meeting national and state legislative requirements including those related to higher education and vocational education and training.

1.2 Purpose

The purpose of this Policy is to provide a framework that ensures the protection of Scentia's ICT Assets from unauthorised access, loss, or damage – while supporting its teaching, learning, and other business needs.

1.3 Scope

This policy applies to all Scentia students and staff including AIM, ABS and ACHW staff, temporary employees, contractors, visitors and third parties globally who manage Scentia information. This policy applies to all business systems, services or applications used to create, manage, and store information, including Scentia endorsed information and records management systems, cloud services and email systems, internal and external websites, social media applications, collaboration applications and databases.

This policy does not override any legal, regulatory, or statutory requirements that Scentia is bound to comply with.

1.4 Scope Exceptions

None

2.0 RESPONSIBILITIES

All Authorised Users of Scentia technology resources have a role to play in information security in accordance with this policy and must be aware of and execute their responsibilities. These include:

1. Understand the information classification levels defined in this policy.

2. As appropriate, classify the information for which one is responsible accordingly.

3. Access information only as needed to meet legitimate business or academic needs.

4. Not divulge, copy, release, sell, loan, alter or destroy any Scentia Information without a valid business or academic purpose and appropriate authorisation.

5. Protect the confidentiality, integrity and availability of Scentia Information and immediately report any suspected breaches of information security.

6. Maintain awareness of the information security risks and controls appropriate to the information accessed and used, including completion of required training as required.

7. Handle information in accordance with Student and Staff Code of Conduct Policy and any other applicable standard, procedure, guideline, or policy.

8. Safeguard any physical key, ID card, computer account, or network account that allows one to access Scentia Information.

9. Managers of employees must ensure correct termination processes are followed to ensure the user account is disabled.

10. Discard media containing Scentia Information in a manner consistent with the information's classification level, type, and any applicable retention requirement. This includes information contained in any hard copy document or in any electronic, magnetic, or other storage medium

11. Contact the Scentia CFO prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

12. Be aware of all legal and corporate responsibilities concerning inappropriate use, sharing or releasing of information to another party. Any third party receiving Restricted Information must be authorised to do so and that individual or their organisation should have adopted information security measures, which guarantees confidentiality and integrity of that data.

3.0 POLICY

Scentia information technology resources are strategic assets that are relied upon for the purposes of course delivery and all administrative and business-related functions and operations. These resources must be appropriately managed and protected to ensure confidentiality, integrity and availability.

4.0 Principles

1. Data Security classifications

All Scentia Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information. When combining information, the classification level of the resulting information must be re-evaluated independently of the source information's classification to manage risks.

Data classification	Description	Examples
Highly Restricted	Data that if breached due to accidental or malicious activity would have a **high** impact on Scentia's activities and may cause serious harm to individuals.	▪ Data subject to regulatory control ▪ Individually identifiable Medical records ▪ Credit card details ▪ Passport numbers ▪ Drivers license details ▪ Passwords, PINs, system credentials and encryption keys ▪ Details of cybersecurity reports, vulnerability assessments, penetration test results
Restricted	Data that if breached due to accidental and malicious activity would have **medium** impact on the Scentia's activities and objectives.	▪ Student records or staff records ▪ Organisational financial data ▪ Examination materials and results ▪
In confidence	Data that if breached due to accidental or malicious activity would have a **low** impact on Scentia's activities and objectives.	▪ Business unit procedures or processes ▪ Contracts ▪ Course and unit performance information ▪ Key performance Indicators
Public	Data that if breached due to accidental and malicious activity would have **insignificant** impact	▪ Faculty and staff directory ▪ Course and unit information

2. Access Management

Logical and physical access to Scentia's information assets must be authorised, controlled, and used in accordance with Scentia policy, as follows:

a. Access to Scentia's information assets and systems is granted by means of an assigned User ID,

b. All Authorised Users are provided a unique User ID to use in accessing systems and applications. User IDs must not be shared and must only be used by the person for whom the ID has been created.

c. Passwords must be changed immediately if there is a suspicion of compromise.

d. Authorised Users are responsible for maintaining the security of their accounts and all activity occurring under those accounts. Knowingly disclosing passwords or other access credentials to others will be deemed a breach of policy and could be referred to disciplinary procedures.

e. Passwords used on all systems should comply with Information and Cyber Security Policy to ensure appropriate protection of Scentia's information assets.

f. Access to Scentia's information assets is granted on the basis of "need to know "and "least privilege", whereby each Authorised User should only be provided access to meet legitimate business needs and is granted the most restricted set of privileges needed for the performance of relevant business tasks.

g. Multi-Factor Authentication is required for remote access to Scentia ICT assets

h. ICT Asset Owners must regularly review their systems to determine who is authorised to use the system and their level of authorisation.

3. Information Asset Management

The protection of Scentia's information, application and technology should be in accordance with the following:

a. Information Assets must not be sent to, exported to, nor stored on a non Scentia computer system, such as a home computer.

b. Information Assets must be appropriately protected when stored, transported, or transmitted.

c. Information Assets must be properly disposed of so that the information cannot be retrieved or reassembled when no longer needed or required to be kept under retention obligations.

d. Information Assets must be stored on Scentia approved storage solutions,

e. ICT and Information Assets must be backed up on a regular basis and backups must be tested periodically to ensure that the procedures followed support full information recovery.

4. Physical Security

a. Access to Secure Areas, including computer rooms, network equipment or communications rooms and any associated service facilities is restricted to authorised staff, through the use of passwords, locks or access-control devices. All wiring closets must be physically secured.

5. Software Security

a. To comply with legislation and to ensure ongoing vendor support, the terms and

b. conditions of all licensing agreements must be adhered to. All software and other applicable materials must be licensed (if required) in an appropriate manner.

c. All software, including patches, upgrades, or new versions, must be tested, archived and documented before being put into Production systems. This transition should be under migration and version control and incorporate appropriate change control procedures.

d. All operational software should have appropriate support in place by the supplier to ensure regular maintenance and adherence to current security standards and compliance with Scentia's Information and Cyber Security Policy.

6. Internet and Third-Party Accessible Security

a. Internet accessible systems must be approved by Scentia IT Team prior to installation on the network.

b. Contracts with vendors that manage ICT Assets must contain specific confidentiality and security language as approved by Scentia CFO

c. In the case of ongoing maintenance and support from 3rd parties, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support.

7. Device Security

a. All devices (including desktops, laptops, servers, virtual machines, and mobile devices such as smartphones and tablets) storing or processing Information Assets must meet the requirements of Scentia's *Information and Cyber Security Manual*

8. Information Security Audits and Monitoring

a. Scentia maintains logs and audit trails of network and system activities which may include personal information about users.

b. The Scentia IT Team performs information security audits and monitoring activities which include the following:

- monitoring its network, information systems, and services against malicious activities, and threats;
- logging and investigating its network, applications, and user activities for the purpose of investigating faults or problems, security breaches, and unlawful activity; and
- regularly auditing the security of information systems

c. Where diagnosis of problems, investigations or security audits are required, Scentia reserves the right to access logs, audit trails and individual files. In carrying out these tasks, cooperation and collaboration with law enforcement authorities may

also be required.

9. Security Breach Notification and Reporting

a. A security breach is defined as any action or event in contravention to the provisions of this Information Security Policy, relevant Scentia policies and applicable State and Federal laws.

b. Any actual or suspected loss, theft, or improper use of or access to confidential information (or a device storing confidential information) must be reported promptly. The responsible officer should take these steps as urgently as possible:

- Scentia CFO and CEO should be notified immediately;
- Follow guidelines containing the Scentia *Information and Cyber Security Manual*
  - If the security breach involves a possible breach of State or Federal law, then the Scentia CFO will notify the Australian Cyber Security Centre or Australian Federal Police (as appropriate), as soon as is practicable;

c. The person authorised by the Scentia CFO, to carry out the technical investigation of a security breach must submit a report outlining the following details (where possible):

- General nature of the security breach;
- General classification of people involved in the security breach, (such as external client, privileged staff member);
- Systems involved in the security breach;
- Details of the security breach;
- Impact of the security breach;
- Unrealised, potential consequences of the security breach;
- Possible courses of action to prevent a repetition of the security breach;
- Side effects, if any, of those courses of action.

d. An assessment will be made by the Scentia CFO as to whether the Australian Computer Emergency Response Team (AusCERT) or other external organisation will be engaged to investigate and assist with remediation.

10. Breach of policy

A proven breach will be managed in accordance with the Student Code of Conduct and Staff Discipline and Termination of Employment policy.

5.0 DEFINITIONS

- **Approved Information Systems** – Refers to systems Scentia uses to manage business operations, and store and manage information and data as part of its business and to meet legislative requirements. These include: Learning Management, Customer Relationship Management, Student Information and Records Management, Finance and HR systems and marketing data.
- **Asset** – means any tangible or intangible item that Scentia owns, or has legal or other right to control and exploit to obtain financial or other economic benefit
- **Authorised User** – means a person who has been provided with credentials to access Scentia ICT Asset /s or Information Asset /s
- **Confidential Information** – means all information which is disclosed to a party by, or on behalf of, the other party, or which is otherwise acquired by a party from the other party, or any adviser engaged by the other party, which:
  - Is by its nature confidential
  - is designated by the other party as being confidential
  - the party knows or ought to know is confidential, but does not include information which:
    1. is or becomes public knowledge other than through a breach of confidentiality;
    2. was already in the possession of a party and not subject to an obligation of confidentiality
    3. is lawfully received from a third party
    4. is independently developed by a party

- **ICT Services**– Any information, communications technology or audio-visual service, equipment or facility owned leased or contracted by the Scentia group that hosts, stores, transmits or presents digital information for the business and purpose of Scentia. This may include, but is not limited to:

  - email, messaging and collaboration applications;
  - any cloud-based facilities associated with the delivery of ICT activities;
  - all hardware and infrastructure (e.g. servers, workstations, voice and data network, wired and wireless networks, audio visual equipment, printers, and portable storage devices);
  - videoconferencing and web conferencing systems, services
  - applications;
  - all software and applications, and services (including but not limited to internet access), and data contained or stored in any ICT facility;
  - Learning Management Systems.

- **Information Asset** - means a body of information, knowledge or data that has value to Scentia

6.0 REFERENCES AND ASSOCIATED INFORMATION

- Code of Conduct Policy (Staff and Students)
- Privacy of Staff Information and Records
- Privacy of Student Information and Records
- Information Management Policy and Procedure

- Student Use of ICT Services Policy and Procedure
- Scentia Risk Management Policy
- Scentia Business Continuity Plan 2021
- Social Media Policy (Staff and Students)
- Staff Use of ICT Facilities Policy and Procedure
- Student Use of ICT Services Policy and Procedure
- Copyright Act 1968 (Cth Australia)
- Crimes Act 1914 (Cth Australia
- Cybercrime Act 2001 (Cth Australia Privacy and Personal Information Protection Act (PIIPA) 1998 No 133
- State and Records Authority NSW
- Telecommunications (Interception and Access) Act 1979 (Cth Australia)
- Tertiary Education and Quality Standards Act 2011
- VET Quality Framework
- NSW State Records Act 1998
- ISO/IEC 27001:2013 - Information Security Management System
- https://www.iso.org/isoiec-27001-information-security.html
- https://www.nist.gov/cyberframework/framework
- https://www.qgcio.qld.gov.au/documents/information-security-policy
- https://www.digital.nsw.gov.au/policy/cyber-security-policy

7.0 POLICY OWNERSHIP

Policy Owner	Head of Technology
Status	New
Approval Authority	Scentia Corporate Board with endorsement of the ABS Corporate Board and ACHW Corporate Board.
Date of Approval	26/04/2023
Effective Date	01/05/2023
Implementation Owner	Head of Technology
Maintenance Owner	Head of Compliance
Review Due	1 March 2026
Content Enquiries	Mike Kumar - Head Technology Email: mkumar@scentia.com.au

8.0 AMENDMENTS

Version	Amendment Approval (Date)	Amendment Made By (Position)	Amendment Details
C33.0	26 April 2023	Head of Technology	New to align with policy suite on Information and data management