ICT Security Policy

1. Purpose	This Policy is in place to ensure that EIA has the ICT security measures in place to safeguard its ICT systems, services and data from potential security threats and assist the institution mitigate any damage or liability arising from the use of the information assets and systems for purposes contrary to the institution's policies and relevant regulatory requirements.
2. Regulatory Alignment	HESF: 2.1 Facilities and Infrastructure; 3.3 Learning Resources and Educational Support; 6.2 Corporate Monitoring and Accountability; 7.1 Representation; 7.3 Information Management The Privacy Act 1988 (Cth) The Australian Privacy Principles Privacy and Data Protection Act 2014 (Vic) The Fair Work Act
3. Scope	This policy applies to all EIA prospective, current and former students, all EIA current and former staff, externals in association with EIA's business, who have access to EIA's ICT assets and data (hereafter referred to as 'users').
4. Policy	
4.1 General	4.1.1 EIA is committed to managing ICT security appropriately, including its information technology infrastructures, services, storing data from unauthorized access, use, disclosure, disruption and modification. 4.1.2 EIA ensures that its governing body has the oversight that the organization's ICT security controls are commensurate with the risks involved. 4.1.3 All users of the EIA's ICT resources and services are responsible for familiarizing themselves with this policy, as appropriate to their role with the institution. 4.1.4 EIA ensures that third party ICT service level agreements, operational level agreements, hosting agreements or similar contracts clearly articulate the level of security required and are regularly monitored.

	4.1.5 EIA ensures the effective response to ICT incidents to maintain secure operations of business.
4.2 ICT Resources and Services	4.2.1 EIA's ICT resources encompasses all technical, electronic and communication systems that serve to assist the operational needs of EIA's business and for students' use in their learning activities. 4.2.2 These resources include those that are owned, leased or otherwise controlled by EIA, and that are used or accessed from the EIA premises. The resources also include the activities through the utilization of EIA paid accounts, subscriptions or other technical services, whether or not the activities are conducted from the EIA premises or elsewhere. 4.2.3 The ICT resources include but are not limited to: a. Desktops and portable computer systems; b. Telephones, wireless devices, mobiles, tablets; c. Internet and web access, voicemail, e-mail, electronic chat rooms, apps; d. Media storage devices, equipment, and systems; e. All hard copies of any communication derived from these ICT resources. 4.2.4 All users must ensure of using EIA's ICT resources and services in a lawful, ethical and responsible manner. EIA retains the right to supervise the use of its ICT resources and services and to deal appropriately with users who breach this policy to use. 4.2.5 All EIA's ICT devices and systems must identify and authenticate users by an approved authentication service. 4.2.6 EIA ensures mechanisms in place to archive the user access from employment onboarding and offboarding. 4.2.7 EIA will not provide ICT services to public users. 4.2.8 EIA will not tolerate its ICT resources being used inappropriately or illegally for the purpose of harassment, discrimination, abuse and threats. Any attempt to use ICT resources to harass, menace, libel, defame, vilify or discriminate against any individual is illegal. 4.2.9 Users who adversely diminish the reputation of another person or EIA may be sued for defamation by that aggrieved person or EIA.

	4.2.10 The IT Support Officer has the authority to conduct a security audit on any system owned by EIA at any time. 4.2.11 ICT security audits may be conducted on all computers and communication devices owned or operated by EIA as well as any computer and communication devices that are present on EIA premise, but may not be owned or operated by EIA, subject to the consent by the owner of the device. 4.2.11 ICT Security audits may be conducted to: a. Ensure integrity, confidentiality and availability of information and resources; b. Investigate possible security incidents; c. Investigate possible violations of laws by which EIA conducts operations; d. Ensure that EIA complies with relevant legislation; e. Monitor user or system activity where there is a legitimate concern that one or more of the above conditions is not being met; f. Ensure resources are used appropriately and for teaching and learning related purposes; and g. Facilitate the recovery of EIA's information stored on individual desktop PCs, laptops or devices.
4.3 Privacy	4.3.1 EIA is committed to protecting personal information through the mechanisms of: a. Having the structured and transparent processes of managing personal information, including keeping updated the privacy policy and procedure, and privacy statement on its website and the applicable documents; b. Giving notice about collection of personal information where applicable; c. Advising how personal information can be used and disclosed; d. Ensuring personal information that it uses or discloses is accurate, up-to date, complete and relevant, having regard to the purpose of the use of disclosure; e. Keeping personal information secure; and f. Providing students and staff with access to and the opportunity to verify and correct their personal information. 4.3.2 EIA's information and databases are restricted to authorized users. Student personal information is held in

	EIA's databases and appropriately secured from misuse, interference and loss and from unauthorised access, modification or disclosure. 4.3.3 EIA will only collect student personal information for the purpose of enrolment and the provision of the education services, such as: a. To respond to a student's queries and requests; b. To keep a record of communication with in order to meeting the legal, regulatory and operational duties; c. To protect EIA and students from fraud and other illegal activities; d. To keep record of a student's academic progress; e. To process payments and to prevent fraudulent transactions; f. To provide information by email, web, text, social media and telephone about relevant services and events; g. To send communications required by law or which are necessary to provide information about EIA's changes to the services the EIA provides; h. To comply with our contractual or legal obligations to share personal information if necessary, as described in Section 4.3.5. 4.3.4 When collecting student personal information, EIA will endeavour to collect the minimum necessary for EIA to provide services. Personal information collected by EIA may include the students' a. Name; b. Residential address; c. Personal Email; d. Telephone number; e. Date of birth; f. Gender; g. Citizenship; h. Passport; i. Visa details; j. Identity card;

k. Emergency contact details;
l. Bank account or other financial details;
m. Educational history, including qualification, academic records, transcripts, English proficiency certificates; and
n. Disabilities or other health information.

4.3.5 Student personal information may only be disclosed:

a. To the Australian Government and designated authorities where the request is justified by law, including to the:
    a) Department of Education, Skills and Employment;
    b) Department of Home Affairs;
    c) Tuition Protection Service;
    d) Tertiary Education Quality and Standards Agency;
    e) State and Federal Police Force;
    f) The external complaints or dispute agencies that students lodge their complaints with;
    g) Educational Agents;
    h) EIA's contracted and professional services providers EIA may enter into arrangements with which may provide a service to students, such as banks, IT provider and health insurance companies.
b. On the reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the student or of other people;
c. To external debt collection agency to recover overdue tuition and non-tuition fees;
d. To EIA's legal advisers or other professional advisers or consultants engaged by EIA;
e. To any third party by which the student provides their authorised consent, such as employment verification organisations or other education providers; or
f. As otherwise required by law.

4.3.6 EIA will only collect and use the staff personal information directly in relation to their employment, including:

	a. Personal and emergency contact details b. Information about terms and conditions of employment c. Wage or salary details d. Leave balances e. Records of work hours f. Records of engagement, resignation or termination of employment g. Information about training, performance and conduct h. Taxation, banking or superannuation details i. Resumes and job related qualification documents j. Union, professional or trade association membership information. 4.3.7 The personal information about unsuccessful job candidates may include the applicants' resumes, contact details, references and academic qualification documents. 4.3.8 EIA will only legally disclose staff records to a third party in some circumstances, for example: a. Information requested by a Fair Work Inspector; b. Information requested by other government agencies or by law; c. Information requested by a permit holder; d. Information requested by an employee or former employee; e. Providing references 4.3.9 When personal information is shared with the third party, the collection and use of the data will be under the terms of that third party's own privacy policy and EIA is not liable for any misuse of that data after it has been passed on to that third party. 4.3.10 The Complaints and Appeals Policy and Procedure may be accessed if people have complaints in respect to their personal information or any potential privacy breaches by EIA. Should matters relating to privacy not be resolved, people may escalate matters to the Office of the Australian Information Commissioner: https://www.oaic.gov.au/privacy/privacy-complaints/.
4.4 Records Management	4.4.1 EIA ensures to have the structured records management in place to: a. Ensure records remain complete, accurate and replicated;

	b. Prevent fraudulent or unauthorised access to information which is deemed confidential or sensitive; c. Ensure that proper records are kept in accordance with the related legal requirements and can be produced when required; d. To help the critical information to be properly identified, tracked and protected, reducing the risk of data breaches, loss of information, or other negative impacts. 4.4.2 All EIA staff are responsible for creating and maintaining accurate records of business that they are engaged in. 4.4.3 All EIA staff must not, under no circumstance damage, destroy, segregate, move or alter any EIA records. 4.4.4 All EIA records will have designated locations of storage and the recorded authorisation of the users to have access to them. This can include physical storage locations, such as filing cabinets, as well as electronic storage locations, such as servers or cloud-based systems. 4.4.5 EIA staff are given access to records that are necessary for their designated roles. Records that contain personal, organisational or operationally sensitive information will have restricted access, whereby only those who are authorised will have access. 4.4.6 EIA will ensure its staff receive updated trainings and clear instructions on records management.
Administrative Details	
Policy Owner	Managing Director
Implementation Officer	Chief Operating Officer
Approved Authority	Board of Directors
Definitions	See EIA Glossary of Terms

Version History

Version	**Approved/Effective Date**	**Amendments**
2.0	26/06/2023	• Integrated the existing ICT Management Policy, Privacy Policy and Records Management Policy into this ICT Security Policy

		• Separated policies from procedures • Added the definition of ICT resources and types of resources • Added the requirements on ICT security audit • Added policy requirements on personal information collection, use and disclosure

Edvantage Institute Australia Pty. Ltd.
ABN: 32 617 256 818 CRICOS Code: 03879J
TEQSA Provider Number: PRV14317