ICT Security Procedure

1. Purpose	The ICT Security Procedure provides the operational processes in support of the ICT Security Policy and should be read in conjunction with the Policy.	
2. Scope	This Procedure 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').	
3. Procedure	The common procedures are shared across the policy requirements on ICT Resources and Services, Privacy and Records Management that EIA abides by for the safeguard of its business operations. The ICT Security Procedure provides guidance on the elements of Access Control, Data Protection, Incident Response and Business Continuity, Auditing and Monitoring, and Training and Awareness.	
Element	**Procedure**	**Key Accountability**
3.1 Access Control	3.1.1 The access in relation to the ICT security at EIA includes physical and technical access. **Physical Access:** 3.1.2 Keys or equivalent access mechanisms to EIA premises are issued only to authorized personnel who require access to the allowed areas. The use of the access mechanisms is logged and managed by the Operations Coordinator, and in liaison with the HR Coordinator in case of staff onboarding and offboarding of their employment with EIA. 3.1.3 Surveillance cameras at the EIA premises are used for legitimate purposes, to ensure staff and students' safety and security, and prevent theft or vandalism. The cameras are visibly installed at the identified risk areas, including entrances, corridors, classrooms and staircases. 3.1.4 The designated staff members have the access to the monitoring system. The IT Support Officer and the Operations Coordinator ensure the footage captured by the cameras is constantly monitored and identify areas for improvement. 3.1.5 Individuals who may be subject to camera surveillance will be clearly notified of the camera's presence and the purpose of the surveillance.	IT Support Officer; Operations Coordinator

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

	3.1.6 Access to physical areas hosting EIA's information assets, such as the server rooms and storages, is controlled to ensure that only authorized staff members, contractors and third-party service providers are allowed access. 3.1.7 Only the IT Support Officer and the Operations Coordinator have access to the server room at the EIA premises, for the maintenance of the servers and/or building infrastructure that supports the servers and/or for the security monitoring.	
	Technical Access 3.1.7 All users shall only use their own assigned login details and shall not give their login details to another person. Any outcomes from such action will be borne by the user. 3.1.8 All users are assigned access to EIA's ICT systems based on their job duties and the security principles of least privilege. The user access will be uniquely identified. 3.1.9 The IT Support Officer must provide approval for new user access to EIA's ICT system with the permission of the department managers through the ICT Services Request Form. The access will be recorded in the ICT Services User Access Register. 3.1.10 The department managers will ensure that when a staff member changes role within EIA, their access will be amended accordingly to reflect the access requirements of their new role. Any user access privileges to business systems that are no longer required for the staff member's new role will be removed. The request for the changes shall be made through the ICT Services Request From and from the line managers. The form will be stored in the HR platform and the changes be reflected in the ICT Services User Access Register. 3.1.11 The IT Support Officer will ensure that staff user accounts are terminated when a staff member leaves employment with EIA and as informed by the HR Department. The removal of the access will be recorded in the ICT Services User Access Register. 3.1.12 Students will continue to have access to their student accounts for a period of 6 months after the end of their enrolment. 3.1.13 EIA management reserves the right to revoke user access at any time. 3.1.14 Contractors will be provided with temporary access for EIA system access with an expiry	All users; IT Support Officer; Department Managers; HR Officer

	date applied in accordance with the contract. 3.1.15 The processes to assign, modify, revoke and revalidate user accounts will be documented and by all means to reduce the risk of unauthorised access to EIA's information assets. 3.1.16 All users must not attempt to repair, interfere with, or add any devices or programs (software, hardware, or any related components) onto any ICT resources unless authorised to do so. The IT Support Officer should be notified of any violations by students or staff. 3.1.17 EIA generated email lists are to be used for internal purposes only and the use of generic user accounts will be strictly controlled. 3.1.18 EIA's shared mailboxes will be strictly managed to ensure smooth operation and efficient handling of emails: a. The creation of the shared mailboxes must be in consistency with the relevant policy requirements; b. Line Managers will determine the individuals who are responsible for managing the shared mailbox and advise the IT Support Officer to grant the appropriate access; c. The access rights will be regularly reviewed and updated by the Line Managers in liaison with the IT Support Officer to ensure that only the necessary individuals have access. 3.1.19 Unless authorised to do so, users must not at any time, facilitate or permit unauthorised personnel to use EIA's ICT resources.	
3.2 Data Protection	3.2.1 Users of EIA's ICT resources must respect and protect the privacy of others; the use EIA's ICT resources to collect, use or disclose any personal, sensitive, confidential or otherwise unauthorised information is not permitted. 3.2.2 Users must not corrupt, destroy or damage data, software or hardware that belongs to EIA or someone else, with the exception of authorised IT staff performing their ICT management duties. 3.2.3 All users should be aware that passwords are often the first line of defense against	All users; IT Support Officer; Student Services

	unauthorised access, and a weak or compromised password can put sensitive information at risk. The IT Support Officer will ensure effective password management and all users have the obligation to follow the IT Support Officer's instructions on password set up and updates. 3.2.4 All users should be aware that emails are a major source for computer malware and have the obligation to follow the IT Support Officer's instructions on email security. 3.2.5 The instructions on the password management and email management will be informed in the Student Handbook and Staff Handbook, and reminded by the IT Support Officer as needed. 3.2.5 All users must keep secure all devices used to access EIA's ICT systems. This includes EIA-issued computing devices as well as personal computing devices such as laptops, tablets and smartphones, used to access EIA's network or storing work-related data. All users shall ensure: a. All computing devices connected to EIA ICT systems must be password-protected, including smart phones; b. Regularly update your operating system, software, browser and antivirus; c. Do not leave your laptop, tablet or phone unattended; d. Lock your screen before leaving your computer, even when leaving for a short time; e. Where possible, make sure that work-related data stored in your portable computing device is fully encrypted; f. If you have to leave your laptop behind, make sure to physically lock it; and g. If your computing device is lost or stolen, notify the IT Support Officer immediately. 3.2.6 Computer malware can easily spread via external storage devices such as thumb drives, external hard drives and Micro SD cards. All users must ensure: a. Scan storage devices before connecting them to your machine; and b. Remove storage devices once no longer in use. You are encouraged to copy the materials you need and unplug the storage device immediately. In which	

	case, make sure to permanently delete the copied materials when no longer needed. 3.2.7 All confidential information must be protected by all users at any time. Confidential information include the personal information described in the ICT Security Policy, EIA's intellectual property such as course materials, management and operations documents, and sensitive information such as wages, financial transactions, health records and exam results. 3.2.8 All confidential information must remain securely stored at any time. The physical documents must be kept in a secure locker which those in digital form must be saved and managed in the designated ICT systems accessed only to the authorised users. 3.2.9 EIA collects student personal information through the enrolment application form which is verified and updated through the orientation process as well as during the student's course of study. 3.2.10 All student must sign a declaration confirming that they understand and consent EIA to use their personal information and appropriate disclosure, as part of their acceptance of the Letter of Offer and Acceptance Agreement with EIA. 3.2.11 An EIA Privacy Statement will be included in the student Acceptance Agreement and EIA will ensure the statement is up to date. 3.2.12 Whenever a student provides EIA with their consent to use their personal information to improve EIA's products and services, they have the right to change their mind at any time and withdraw that consent. 3.2.13 EIA ensures that individual student personal information is up to date and will request students to provide their latest personal information where there are changes. The student personal information will be updated in a timely manner in the Student Management System by the Student Services. 3.2.14 Students may request access to their personal information by contacting Student Services. The student will be asked to state their past contact details for verification	

	purposes before the records are amended. There are no fees for students to access their personal information. 3.2.15 EIA will respond to external requests for access to students' personal information, and they will do so within a reasonable time after receiving the request. If an external request is legally made, EIA is not required to notify the student. 3.2.16 Student records which are no longer required will be appropriately destroyed in accordance with the appropriate legislative requirements.	
3.3 Incident Response and Business Continuity	3.3.1 When data breach occurs, EIA ensures to respond quickly and effectively to minimize the damage and prevent further unauthorised access. 3.3.2 The sources of the breach and the content of the data will be identified as quickly as possible. Action will be taken in accordance with the situation, including but not limited to taking the affected systems offline, blocking unauthorised access; and/or isolating the compromised data. 3.3.3 Once the breach has been contained, EIA will notify the relevant stakeholders immediately. This may include the IT Support Officer, related managers, affected students and/or staff, the governing bodies, and legal consultants. Such communication will be conducted in a timely and transparent manner and providing accurate information about what happened and what steps EIA will take to mitigate the damages. 3.3.4 EIA will conduct a thorough assessment of the breach to determine the scope and extent of the damage. This may involve reviewing logs, analysing system activities, and conducting forensic investigations. 3.3.5 Following the assessment, corresponding steps will be taken to mitigate the damage caused by the breach, such as restoring data from the backups, repairing systems and implementing additional security measures to prevent future breaches. 3.3.6 A post-incident review will be conducted after the data breach is remediated, including but not limited to: a. Evaluating the response process to the breach;	All users; Managing Director

	b. Identifying the weaknesses and gaps in the EIA's security measures; and c. Implementing changes to prevent similar breaches in the future. 3.3.7 The whole process of data breach and EIA's response to the breach will be documented in detail.	
3.4 Auditing and Monitoring	3.4.1 EIA reserves the right to access to users' accounts, the content of electronic communications and the documents transmitted through and stored on any of the EIA work related ICT resources. 3.4.2 EIA maintains the right to audit regularly and monitor the use of its ICT resources to ensure compliance. 3.4.3 EIA will conduct regular ICT security risk assessment and update the assessment to the Board of Directors for oversight. The assessment includes the likelihood and impact of potential threats, and identifying areas where additional controls are needed. 3.4.4 EIA will conduct regular ICT security audit to ensure that the ICT Security Policy is implemented effectively and to identify any gaps in the system. The audit may include conducting vulnerability assessment, penetration testing and compliance audit. 3.4.5 The audit will be conducted by the IT Support Officer. The audit report will be submitted to the Management for review and for actions to take where needed. Management will report to the Board of Directors on the report and the actions for the governance oversight.	IT Support Officer; Managing Director; Board of Directors
3.5 Training and Awareness	3.5.1 Regular ICT security training sessions will be conducted to ensure that they are aware of EIA's ICT security requirements and processes. The training sessions will also educate the staff members on the potential security threats and their roles in them. 3.5.2 The training session will take the following steps to ensure the effectiveness: a. The training needs will be identified based on the staff's knowledge level and skills on ICT security; b. The materials and forms of the training sessions will be developed, which may include training modules, presentations and hands-on exercises; c. The training schedules will be established at regular intervals or as part of new employee onboarding process;	IT Support Officer: Chief Operating Officer

		d. Follow-up resources will be provided, such as reference materials, to reinforce the training and encourage ongoing learning; e. The training's effectiveness will be evaluated by collecting feedback from the staff members. The feedback will be used to improve the future trainings; f. The training materials will be updated to reflect changes in security threats and technology.	
Administrative Details			
Procedure Owner		Managing Director	
Implementation Officer		Chief operating Officer	
Approved Authority		Managing Director	
Definitions		See EIA Glossary of Terms	
Version History			
Version	**Approved/Effective Date**	**Amendments**	
2.0	26/06/2023	• Classified the common ICT security elements on matters of ICT resources and services, privacy and records management into access control, data protection, incident response and business continuity, auditing and monitoring, and training and awareness • Detailed procedures developed for the above elements	