Information Management and Security Policy

1 Scope and Purpose

This policy applies to all staff of Russo Business School higher education community.

Russo Business School's relationship with accrediting and registration bodies requires a number of information security measures to be achieved and adhered to. RBS is a part of the Sarina Russo Group (SRG) and whilst as a group we have in place robust controls overseen by our in-house Information Technology (IT) team, the SRG has created an organisational culture which sees all employees sharing in this responsibility.

Globally there is a growing awareness that information assets (which includes personal information and other data) are subject to cyber threats. These attacks are increasing in sophistication and frequency.

It is therefore the priority of the Sarina Russo Group and Russo Business School to ensure we maintain a safe, trusted and resilient operating environment to mitigate potential threats.

Of additional importance is the overall management and maintenance of our Student Management System (eBECAS). This system contains sensitive student data to support; admission, enrolment and generation of Academic Records of each admitted student past, present and future.

2 Definitions and Abbreviations

Duty of care Russo Business School's duty of care requires all Staff, Affiliates and Students to take reasonable care in order to avoid reasonably foreseeable harm that may arise. The safety and wellbeing of Staff, Affiliates, Students and visitors is the first priority in any situation.

CISO Chief Information Security Officer

3 Policy Objectives

To support our commitment to Information and cyber security, SRG and RBS have policies, procedures, standards, contracts and controls to address information security management across all operations.

This policy is designed to cover the key elements of Information Security, these being:

- Access to information
- Asset management
- Supplier Relationships
- Systems Management and maintenance
- Physical and Environmental Management
- Information Security Incident Management

- Retention of Records
- Clean Desks and Clear Screens

It is to be noted that all Sarina Russo Group Information Security Polices, Standards and Procedures are to be referenced as they support this policy.

The purpose of this policy is to provide RBS with appropriate guidance in developing and endorsing controls in the context of protecting information and technology assets from information and cyber security related risks.

3.1 Access to information

The purpose of access management is to ensure the implementation of access controls for RBS information systems and network resources that will reduce the risk of accidental or deliberate destruction of data and protect it from unauthorised dissemination. The intent is to limit access to information and information processing facilities.

Access management consists of:

- Access Control – This domain includes all activities that set access and control policies.
- Authentication – This domain includes all activities and measures that ensure users are the persons they claim to be.
- User access – This domain includes all activities that ensure authorised access to information and applications. Private or sensitive information, including information where unauthorised access may compromise academic or research integrity
- User responsibilities – This domain includes all activities that ensure users understand their responsibilities to prevent unauthorised access, compromise or theft of information and IT assets.
- Network access – This domain includes all activities that ensure network access is restricted to authorised users.
- Operating system access – This domain includes all activities that ensure access to operating systems is restricted to authorised users.
- Application and information access – This domain includes all activities that ensure access to information and applications is restricted to authorised users.
- Mobile computing and teleworking – This domain includes all activities that ensure information security is maintained when using mobile computing and telework facilities

Access to SRG information and system resources must be based on least user access that is specific to each individual's role and responsibilities. All such access must be authorised by the Information Owner or their delegate who is responsible for the system, application or data with the amount of detail and the strictness of the controls reflecting the associated information security risks.

3.2 Asset management

The purpose of information asset management is to ensure RBS can determine what assets are, where they are, who owns them, their level of importance to the organisation, to then inform the application of security controls to protect information assets based on a prioritised approach.
Asset management consists of:
Asset protection responsibility – this domain includes all activities that implement and maintain appropriate protection of organisational assets.
Information security classification – this domain includes all activities that ensure information is appropriately classified.

In order to protect the assets of the organisation the following controls must be put in place. RBS must identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information must include creation, processing, storage, transmission, deletion and destruction. Documentation must be maintained in dedicated or existing inventories as appropriate.

3.3 Supplier Relationships

Users of RBS information systems are required to understand and comply with the SRG Supplier Relationship Standard and report suspected breaches. The Chief Information Security Officer (CISO) will monitor compliance

3.4 Systems Management and maintenance

In order to protect the assets of the organisation, RBS must identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information must include creation, processing, storage, backup, transmission, deletion and destruction. Documentation must be maintained in dedicated or existing inventories as appropriate.

Systems acquisition, development and maintenance consists of:

- System security requirements – This domain includes all activities that ensure security requirements are articulated during the development of new systems, or when planning enhancements to existing systems.
- Correct processing – This domain includes all activities that prevent errors, loss, unauthorised modification or misuse of information in systems.
- Cryptographic controls – This domain includes all activities that protect the integrity, confidentiality and authenticity of information by using cryptographic controls.
- System files – This domain includes all activities that ensure system files are adequately protected, including processes for backed ups either physically or in the cloud
- Secure development & support processes – This domain includes all activities that ensure the ongoing security of applications.
- Technical vulnerability management – This domain includes all activities that reduce risks arising from the exploitation of technical vulnerabilities.

The CISO must be advised of all new systems, applications and suppliers providing IT services prior to their development or contractual engagement. Once informed, a security risk analysis of the new system, application, or supplier must be performed using a formalised process, to ensure that appropriate security controls are identified and incorporated during the development or procurement process

3.5 Physical and Environmental Management

The security and protection of SRG assets, facilities and personnel are fundamental to the efficient and effective operations of the organisation. Information computing (servers, laptops and workstations) and mobile (smartphones, tablets) devices issued by SRG are the organisation's assets and must be adequately protected from theft, loss and unauthorised access. Security perimeters must be defined and used to protect SRG facilities and areas that contain either restricted or confidential information.

Physical and environmental management consists of:

- Building controls and secure areas – This domain includes all activities that ensure confidential information assets are not compromised by unauthorised physical access, damage or interference to premises or information.
- Equipment security – this domain includes all activities that ensure information assets are appropriately classified and handled.

It is important to ensure the protection of RBS confidential information assets, facilities and personnel whether in the office, teleworking, at operational sites or traveling. Protecting the availability, confidentiality and integrity of confidential information assets that reside within RBS is critical. The theft or misuse of information or assets could lead to operational, financial and other impacts for the organisation, and damage to RBS's reputation.

3.6 Information Security Incident Management

SRG and RBS depends on the confidentiality, integrity, and availability of its information assets to successfully conduct its business and meet customer and business partner expectations. SRG and RBS recognises that intentional and unintentional events such as unauthorised access, computer viruses, improper escalation of privileges, loss and or theft of organisation assets, by disgruntled internal users and/or external threat agents can breach the Information Security of the organisation. In order to minimise the potential impact and limit the damage, in the case of such an event occurring, the organisation must respond quickly and effectively. The purpose of an Information Security Incident Management Standard is to ensure SRG and RBS can properly identify and handle incidents that affect confidentiality, integrity and availability of the information assets of the organisation.

3.7 Retention of Records

Student records retention and destruction to be aligned with the SRG Retention of Records Policy

3.8 Clean Desks and Clear Screens

SRG has developed a Clear Desk and Clear Screen Standard to reduce the risk of unauthorised access, modification or loss of the information whether in digital or physical format, and whether inside or outside the corporate environment.
The purpose of the policy is to establish the minimum requirements for:

- maintaining a "clear desk" where restricted/confidential information about our employees, intellectual property, customers and our vendors is secure in locked areas and out of site.
- ensuring that the contents of the computer screen are protected from prying eyes and the computer is protected from unauthorised use

4 Implementation

Russo Business School will ensure that records are managed according to this policy and meet all regulatory requirements. The following principles apply:

a. All records are true and accurate
b. All records are accessible for the relevant business contexts
c. All management system records are the responsibility of the personnel listed in the Retention Schedule at Appendix 1 of the RBS Records Management Policy
d. All student information is confidential and is only made available to the students themselves; to a person authorised by them; or when ordered to do so by a legal requirement.

4.1 Privacy and confidentiality

All student and staff records are subject to privacy and confidentiality requirements as generally applicable in Australian Law. A basic principle is that personal information for students or staff may not be accessed without their written consent and that individual staff and students have a right of access to their personal file.

5 Procedure

There are no related procedures

6 Related Documents

Legislation and Standards

Educational Services for Overseas Students Act 2000 (ESOS Act)
Higher Education Standards Framework (Threshold Standards) 2021
Higher Education Support Act 2003 (HESA)
Information Privacy Act 2019 (QLD)
National Code of Practice for Providers of Education and Training to Overseas Students 2018
Privacy Act 1988

The following policies and procedures are related to this policy:
SRG Access Management Policy
SRG Asset Management Policy
SRG Supplier Relationship Standard
SRG Information Security Incident Management Standard
SRG Retention of Records Policy
SRG Clear Desk & Screen Standard
SRG Electronic Use Policy
SRG Telecommunications Policy
SRG Info-Byte Series

RBS Critical Incident Policy and Procedure
RBS Privacy Policy
RBS Records Management Policy
RBS Student Complaints & Appeals Policy and Procedure

7 Review

Three years from commencement.

8 Accountabilities

Delegated Authority	Delegation
Governance	
Board of Directors	Refer to the Terms of Reference
Academic Board	Refer to the Terms of Reference
Learning and Teaching Committee	Refer to the Terms of Reference
Executives	
Executive Dean	Relevant to Accountability Statement

Management	
Dean of Studies	Relevant to Accountability Statement
Manager Standards and Operations	Relevant to Accountability Statement
Chief Information Security Officer (CISO)	Relevant to Accountability Statement

9 Revision History

Policy & Procedure Version No	Policy & Procedure Sponsor	Approval Authority	Date of Approval	Date for next review
1/2022	Chief Operating Officer	Board of Directors	13/07/2022	13/07/2024