Prudential Supervision Policy Statement No: 2

MINIMUM REQUIREMENTS FOR THE MANAGEMENT OF CYBERSECURITY RISK BY SUPERVISED ENTITIES

NOTICE TO LICENSED COMMERCIAL BANKS, CREDIT INSTITUTIONS, INSURANCE COMPANIES, INSURANCE BROKERS, SECURITIES EXCHANGE, MANAGEMENT COMPANIES OF MANAGED INVESTMENT SCHEMES, STOCK BROKERS, FIJI NATIONAL PROVIDENT FUND, FIJI DEVELOPMENT BANK, AND RESTRICTED FOREIGN EXCHANGE DEALERS

Reserve Bank of Fiji
03 March 2023

PART 1: PRELIMINARY

1.0 Introduction

1.1 This Policy is issued pursuant to:

a) Section 14(3) of the Banking Act 1995;
b) Section 3(2) (a) of the Insurance Act 1998;
c) Section 9(2) (c) of the Reserve Bank of Fiji Act (Cap.210);
d) Legal Notice 88 of 2002 Delegation of Powers and the Exchange Control Act 1985;
e) Section 3(1) (a) of the Reserve Bank of Fiji (Capital Markets and Securities Industry) Regulation 2015; and
f) Section 119 (1) of the Fiji National Provident Fund Act 2011.

This Policy applies to all licensed commercial banks, credit institutions, insurance companies, insurance brokers, securities exchange, and management companies of managed investment schemes, stock brokers ,the Fiji National Provident Fund, Fiji Development Bank, and Restricted Foreign Exchange Dealers, hereinafter referred to collectively as **"Supervised Entities"** (SEs), for the purposes of this Policy.

1.2 In the case of branches of foreign incorporated SEs, the requirements of the Policy will apply to the board's delegated authorities responsible for the branch in Fiji, and the senior management of the branch.

1.3 In issuing the requirements of this prudential Policy statement, reference has been made to the relevant standards and guidance issued by global standard setters, and similar requirements of selected supervisory authorities.[1]

2.0 Background

2.1 Cyber risk often stems from malicious intent, and a successful cyber attack, unlike most other sources of risk can shut down a SE immediately, and lead to system wide disruptions and failures. The probability of attack has increased as financial systems have become more reliant on information and communication technologies, and as threats have continued to evolve.

2.2 Cybersecurity refers to the controls and processes put in place to preserve the confidentiality, integrity and availability of information assets. A weak cybersecurity risk management framework has the potential to negatively influence public confidence in the safety of the financial system, if not effectively mitigated.

[1] Bank of International Settlements (BIS), the International Monetary Fund (IMF), International Organisation for Standardisation (ISO), International Telecommunications Union (ITU) and Information Systems Audit and Control Association (ISACA), and similar requirements of selected supervisory authorities.

2.3 Effective cybersecurity enhances the risk management capacity of SEs in many ways, but are not limited to the following:

g) protection against worms, viruses, spyware and other unwanted programs;

h) protection against data theft via implementation of high-security protocols;

i) protection of the system from being compromised by unauthorised users; and

j) breach of data and system privacy.

3.0 Objectives of the Policy

3.1 The financial sector is highly, and increasingly, dependent on information and communication technologies (ICT). A cyber attack can disrupt the provision of critical functions, threaten liquidity, and destabilise the integrity of the financial system.

3.2 This prudential Policy statement therefore aims to ensure that SEs have in place a robust cybersecurity risk management framework, commensurate with the complexity of their operations and the assessed level of cyber risk inherent in their operations. The Policy further seeks to ensure that cybersecurity incidents are minimised within the SE’s risk tolerance levels.

3.3 Cybersecurity practices vary between SEs, contingent upon a scope of variables including size, unpredictability of activity, hierarchical structure, proprietorship structure, nature and extent of budgetary allocation, corporate methodology and risk profile. Notwithstanding these variables, the first line of defence against cybersecurity risk rests with the financial institutions’ own risk management, and each SE should establish and implement a suitable and sound cybersecurity environment, with an effective administration of cyber risk culture.

PART 2: REQUIREMENTS OF THE POLICY

4.0 Cybersecurity Governance Framework

4.1 The board is ultimately responsible for ensuring that cybersecurity is effectively embedded in the SE’s operations at all times. As part of a comprehensive cybersecurity governance framework, a SE must:

a) establish and maintain a comprehensive and effective Cybersecurity Risk Management Framework (CSRMF);

b) clearly define the cybersecurity related roles and responsibilities of the board, senior management, governing bodies, and individuals;

c) maintain a cybersecurity capability, commensurate with the size and extent of threats to its information assets;

d) implement controls to protect its information assets, in line with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls;

e) minimise the likelihood and impact of cybersecurity incidents on the confidentiality, integrity or availability of its information assets, including information assets managed by related parties or third parties; and

f) ensure that the board and senior management fully recognise the extent to which their institutions have complied with the requirements of this Policy, and take adequate steps to improve the SE's practices.

4.2 Cybersecurity Risk Management

4.2.1 A SE must have in place a documented CSRMF that is part of its enterprise risk management framework, board approved, and is regularly reviewed. A comprehensive and effective CSRMF must at a minimum include:

a) clear definitions of the elements of cybersecurity governance such as organisation structures, roles and responsibilities, and reporting lines;

b) a formally documented statement of the board's cybersecurity risk tolerance;

c) cybersecurity risk assessment methodology and tools;

d) cybersecurity processes which considers identification, protection, detection, response and recovery functions;

e) process for reviewing the effectiveness of the framework, together with the relevant improvement and learning process; and

f) the three lines of defence of risk management for cybersecurity.

4.2.2 Subsidiaries or branches may adopt the relevant requirements of their parent's CSRMF, but the minimum requirements of this Policy must be effectively complied on a stand-alone basis.

4.2.3 Essential to a robust CSRMF are effective cybersecurity risk management functions. SEs must establish a designated cybersecurity risk management function that at a minimum:

a) is responsible for assisting the board, board committees and senior management of the institution to maintain its CSRMF;

b) is appropriate to the size, business mix and complexity of the SE;

c) has independent reporting lines to the board and relevant board committees, so as to conduct its risk management activities in an effective and independent manner;

d) is resourced with staff who possess appropriate experience and qualifications to exercise their responsibilities;

e) is headed by a person designated as the Chief Information Security Officer (CISO) or an equivalent senior officer of the SE;

f) implement risk assessment methodology and tools; and

g) operationalise cybersecurity processes including identification, protection, detection, response and recovery functions.

4.3 Cybersecurity Strategy

4.3.1 As part of its CSRMF, a SE must develop and document an enterprise wide cybersecurity strategy (CSS), approved by the board.

4.3.2 The strategy, at a minimum, must:

a) outline the cybersecurity risks and challenges faced by the SE;
b) explain the SE's overall approach to cybersecurity risk management and how this aligns to the SE's overall business strategy;
c) include key elements of the SE's cybersecurity risk management objectives, principles and implementation;
d) be aligned with the board's established and documented cybersecurity risk tolerance levels; and
e) establish a plan for cybersecurity risk management to identify, assess and control cybersecurity threats covering people, policies, processes and technologies.

4.3.3 A SE must conduct regular reviews of its cybersecurity strategy to ensure the strategy remains relevant and current to the SE's overall business strategy, risk tolerances and its operations in the internal and external environment.

4.4 Cybersecurity Policy

4.4.1 A SE must have in place a cybersecurity policy commensurate with its exposures to vulnerabilities and threats, covering policies and procedures for cybersecurity risk identification, measurement, monitoring and control.

4.4.2 Cybersecurity policies and procedures must cover requirements arising from the SE's business strategy, regulatory framework and the current and projected cybersecurity threat environment.

4.4.3 The cybersecurity policy should cover at a minimum requirements for the SE's:

a) information asset management;
b) access control;
c) physical and environmental security;
d) end user management;
e) cryptography;
f) operations security;
g) communication;
h) system development;
i) third-party relationships;
j) incident management;
k) business continuity; and
l) regulatory compliance.

4.4.4 SEs should review and update their cybersecurity policies and procedures at least annually, or when major changes occur in their security and general operating environment.

4.5 Roles and Responsibilities

4.5.1 The board and senior management of a SE must ensure that a sound and robust CSRMF is established and maintained. The board is ultimately responsible for the institution's CSRMF, and the oversight of its operation by management, and must, inter alia:

a) approve the CSRMF;
b) approve the CSS;
c) set and formally document the cybersecurity risk tolerance levels;
d) approve cybersecurity policies and procedures;
e) ensure receipt of information on the cybersecurity risk profile of the institution, including significant cyber security incidents; and
f) ensure the CSRMF is subject to effective and comprehensive audits and testing.

4.5.2 Senior management is responsible for implementing and maintaining the CSRMF consistent with the board's cybersecurity risk tolerance through:

a) ensuring sufficient resources are available for the effective operation of the cybersecurity risk management framework;
b) ensuring that relevant cybersecurity policies and procedures are clearly communicated throughout the SE;
c) maintaining a process of continuous assessment of the institution's cybersecurity risk profile and associated periodic reporting;
d) periodically reviewing, assessing and enhancing the effectiveness of the CSRMF; and
e) establishing the SE's CSS.

4.5.3 The Chief Information Security Officer (CISO) (or equivalent) is responsible for:

a) developing and enhancing the CSRMF;
c) ensuring the consistent application of policies and standards across all technology projects, systems and services;
d) providing leadership to the SE's cybersecurity organisation;
e) partnering with business stakeholders across the SE to raise awareness of cybersecurity risk management concerns; and
f) assisting with the overall SE's technology planning, providing information on current threats and the future vision of technology and systems.

4.5.4 The internal audit function of the SE is responsible for conducting periodic cybersecurity risk assurance audits, and this should include testing of the cybersecurity environment of the SE.

4.5.5 The compliance manager is responsible for conducting assessments of the compliance of the SE to its cybersecurity risk policy framework, and to the requirements of this policy.

5.0 Human Resources

5.1 Screening and Background Checks

5.1.1 People are the first line of defence when it comes to protecting data and systems. SEs must have a comprehensive screening and background checking process for prospective employees and contractors, which covers relevant laws and regulations.

5.1.2 SEs must document policies and controls regarding recruitment and hiring of personnel (including employees and suppliers), identity and access management, and implement controls such as segregation of duties, employee mobility, transfers, and leave.

5.1.3 The screening and background checking process of the SE should be proportional to the business requirements, sensitivity of the information to be handled, and the perceived risks.

5.2 Necessary Competence

5.2.1 SEs must have employment guidelines to ensure that all employees hired for cybersecurity related roles have the necessary skills and experience to perform the role in a trusted, competent manner.

5.3 Security Awareness Program

5.3.1 SEs must have a cybersecurity awareness and training program to ensure that all employees and contractors are aware of their responsibilities for cybersecurity, and how these responsibilities are to be discharged.

5.3.2 The cybersecurity awareness and training program must encompass the entire range of target audiences, including employees, managers, developers, system and infrastructure administrators, external entities, suppliers and customers.

5.3.3 Cybersecurity awareness training should be conducted at least annually, during the onboarding of employees, and when employees are transferred to a new position or roles with substantially different cybersecurity requirements.

5.4 Contractors

5.4.1 SEs must have a policy and written guidelines on engaging contractors to critical information technology operations and cybersecurity functions. The guidelines at a minimum must include:

a) screening and background checks;
b) communication protocols;
c) terms and conditions of the engagement;
d) compliance to the institution's code of conduct;
e) confidentiality and non-disclosure agreements; and
f) fit and proper criteria.

6.0 Asset Management

6.1 Asset Inventory and Ownership

6.1.1 SEs must ensure that all information, information processing and communication assets are identified and inventoried. The inventory of these must be maintained accurately.

6.1.2 Ownership of information assets maintained in the inventory must be appropriately assigned. The asset owners should:

a) define protection requirements for the assets owned, be accountable for these protection requirements and ensure regular review; and
b) identify assets critical to the continued operation of the SE to ensure commensurate protection.

6.2 Information Classification

6.2.1 SEs must define and have in place a board approved information asset classification scheme. The classification scheme, at a minimum, must:

a) include confidentiality, integrity, and availability requirements for each category; and
b) have institution wide applicability.

6.2.2 Information assets that are in the highest protection category, at a minimum, should be labelled regardless of their format (physical or electronic).

6.3 Media Handling

6.3.1 SEs must have appropriate policies and procedures in place to prevent unauthorised access, modification, removal or destruction of media used for the storage of information assets.

7.0 Access Control

7.1 Principles of Access Control

7.1.1 SEs must establish, document and implement relevant policies and procedures to control access to information assets, and information processing and transmitting facilities.

7.1.2 The policies must at a minimum include:

a) information dissemination and authorisation (for example the “need to know” and “default deny” principles, cybersecurity levels and classification of information);

b) application of segregation of duties principles commensurate with the size and complexity of the SE’s operations, and the risk level of the operations and functionalities involved; and

c) clearly defined roles and responsibilities.

7.2 User Access Management

7.2.1 SEs must establish, document and implement relevant policies, and procedures to address the following:

a) user identification (ID) (account) lifecycle management including creation, modification, suspension and deletion of user identities;

b) access rights lifecycle management, including requesting, approving, granting, changing and revoking access rights;

c) appropriate recording of audit trails for all access rights related activities;

d) user IDs and access rights activities must be regularly (at least annually) reviewed and any discrepancy with policies promptly followed up, resolved and appropriately reported;

e) requirements for secret authentication information for all user IDs compliant with defined and enforced complexity requirements and expiration times, that effectively mitigate the risk of uncovering them;

f) requirements for privileged access rights assigned to user IDs different from those used for regular business or ICT related activities must include:

(i) the number of user IDs with privileged access rights must be kept at the minimum possible;

(ii) to the extent possible privileged user ID must be set up with strong (i.e. two-factor or three-factor) authentication;

(iii) activities performed using privileged access rights should be subject to close monitoring; and

(iv) requirements for the use of generic administration user IDs limiting usage to the extent possible.

8.0 Cryptography

8.1 Use of cryptography to protect sensitive data

8.1.1 SEs must develop and implement a comprehensive policy on the use of cryptography for protection of confidentiality, authenticity and integrity of information. The policy at a minimum must include:

a) senior management’s approach towards the use of cryptographic controls across the institution;

b) use of encryption (e.g. end-to-end encryption) and authentication measures on a risk-based basis to safeguard data during transmission across open and public networks as per the institution's classification scheme on criticality and sensitivity of information;

c) the use of encryption for protection of information transported through devices and equipment;

d) methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised and damaged keys; and

e) vetting functions involving cryptographic algorithms and crypto-key configurations for deficiencies and loopholes.

8.2 Key Management Policy

8.2.1 SEs must develop and implement key management policy to ensure that cryptographic keys are secure through their whole life cycle. The policy at a minimum must include:

a) methods for generating keys for different cryptographic systems and different applications and disposal of materials used in the generation of keys;

b) hardware security modules and keying materials are physically and logically protected;

c) procedures for issuing and obtaining public key certificates;

d) storing keys, including how authorised users obtain access to keys;

e) procedures on exchanging or updating keys upon expiry, including rules when keys should be changed and how this will be done;

f) dealings with compromised keys, revoking keys, lost keys and backing up or archiving keys; and

g) when cryptographic keys are being used or transmitted, the SE should ensure that these keys are not exposed during usage and transmission.

8.2.2 Cryptographic keys should be used for a single purpose, to reduce the impact of an exposure of a key, and SEs should consider and decide the appropriate lifetime (validity period) of each cryptographic key.[2]

9.0 Physical and Environmental Controls

9.1 Physical Security of Information Processing Facilities

9.1.1 SEs must define security perimeters to protect areas that contain sensitive or critical information and information processing facilities.

9.1.2 Physical and logical access to data center and systems should be permitted only for individuals who are identified and authorised, and authorisation should be limited only to those with a legitimate business need for such

[2] The sensitivity of data and operational criticality should determine the frequency of key changes.

access according to job responsibilities. Physical access of staff to the data center should be revoked immediately, if it is no longer required.

9.1.3 SEs must ensure that there is proper notification of, and approval for third parties who require temporary access to the data center, to perform maintenance or other approved work, and that visitors or third parties are accompanied at all times by an authorised employee while in the data center.

9.1.4 SEs must ensure that the data center building, facility, and equipment room are physically secured and monitored at all times, and deploy security systems and surveillance tools, as appropriate.

9.2 Physical Entry Controls

9.2.1 SEs must ensure secured areas are protected by effective entry controls that only allow access to authorised personnel at all times.

9.2.2 SEs must maintain a physical logbook for recording physical movements in the data center for all personnel access, including information technology personnel, visitors and third parties. The log book should be reviewed regularly for suspicious cases.

9.2.3 The access rights to the data center should be regularly reviewed and updated, and revoked when necessary.

9.2.4 SEs should conduct spot checks on the physical security of their information processing facilities and verify that adequate physical security measures are implemented at third-party payment kiosks, which accept and process the SEs payment cards.

9.3 Equipment Protection

9.3.1 SEs must have adequate controls in place for equipment and devices issued to employees to prevent loss, damage, theft or compromise of equipment and devices and interruption to the institution’s operations.

9.3.2 SEs should also have adequate controls in place for:

a) maintenance of the equipment and devices;
b) removal of equipment and devices;
c) security of equipment and devices off-premises;
d) secure disposal or re-use of equipment and devices; and
e) unattended user equipment and devices.

9.4 Clear Desk Policy

9.4.1 SEs must implement a clear desk policy for all personnel that includes papers and removable storage media.

9.4.2 SEs must have a clear screen policy for at least the information processing facilities.

10.0 Operations Security

10.1 Operational Procedures and Responsibilities

10.1.1 SEs must have formal documented procedures for operational activities relating to information processing and communication facilities; including:

a) computer start-up and close-down procedures;
b) equipment maintenance;
c) operation and management of media; and
d) mail management.

10.1.2 Operational procedures should clearly identify management responsibilities and controls over all changes relating to information processing and communication facilities.[3]

10.1.3 SEs must implement appropriate monitoring systems for the use of all information technology resources, to ensure effective operational control of information processing and communication facilities.

10.1.4 To ensure sufficient operational capacity, SEs must monitor the volume of use of information processing and communication facilities and project and manage future capacity requirements.

10.1.5 Commensurate to the level of risks inherent in their information systems, SEs must ensure that there is an adequate segregation and separation of duties for systems development, testing and operational environments.

10.2 Malware Protection

10.2.1 SEs must ensure that all information processing and communication facilities have up-to-date malware protection mechanisms.

10.3 Back Up

10.3.1 SEs must maintain information backup facilities, ensuring that significant information and software can be recovered following an operational failure, disruption or disaster. Backup duplicates of data, applications, and system images are to be tested regularly, in accordance with documented and approved backup policies and procedures.

10.3.2 SEs must ensure that the backup policy and procedures are based on defined data loss tolerances and recovery requirements and address retention and protection requirements.

[3] In this regard, SEs should maintain a register of these changes.

10.3.3 Backup facilities must be accessible at a remote location that is unlikely to be affected by the same operational failure, disruption or disaster event as the main operations site.

10.3.4 In cases of critical assets, backups must cover all information necessary for a comprehensive recovery in the event of an operational failure, disruption or disaster.

10.4 Logging and Monitoring

10.4.1 SEs must keep and regularly review event logs that record user activities (including system administrators), exceptions, faults and cybersecurity events.

10.4.2 Event logs must:

a) be protected against unauthorised access, tampering, and data loss (including by system administrators); and

b) be subject to privacy controls.

10.4.3 SEs must ensure all clocks of data processing and communication services are automatically synchronised to a single reference time source.

10.5 Software Installation

10.5.1 SEs must have in place documented policies and procedures to control changes to software on operational systems. All installation and systems upgrades and updates must be assessed, approved, implemented and reviewed in a controlled manner, in accordance with documented policies and procedures.

10.5.2 SEs must have stated strategies and plans for 'Software System End of Life' and adopt and enforce policies to control the types of software and updates users may install.

10.6 Vulnerability Management

10.6.1 Information about technical vulnerabilities of information systems must be obtained in a timely fashion. The SE's exposure to such security vulnerabilities are to be evaluated and appropriate measures implemented to address the associated security risks.

10.6.2 SEs must establish the roles and responsibilities associated with vulnerability management, including vulnerability monitoring, vulnerability risk assessment and the installation of security updates.

10.6.3 SEs should install all relevant security updates to software on operational systems without undue delay and prioritising high risk systems, and must test and evaluate these security updates before installation on critical systems, for effectiveness and undesired side effects.

10.6.4 If installing a security patch would result in side effects that cannot be tolerated, or a security update is not available, then compensating controls must be implemented to mitigate the resulting exposure.

11.0 Communications Security

11.1 SEs must have in place controls to ensure the security of information in networks and the protection of connected services from unauthorised access, including:

a) documented and approved responsibilities and procedures for the management of networks;
b) controls to ensure confidentiality and integrity of data transmitted over networks not controlled by the institution, or wireless networks;
c) restrictions on system connections to the networks; and
d) authentication of systems on the network.

11.2 Network services' security mechanisms, service level requirements and required management services, must be identified and be subject to documented service level agreements, whether services are provided internally or outsourced.

11.3 SEs deploying Wireless Local Area Networks (WLAN) must take measures to mitigate the risks associated with this environment, such as having secure communication protocols for transmissions between access points and wireless clients.

11.4 Groups of users and information systems must be segregated based on an assessment of the security requirements of each group, and access between such segregated groups and between the SE's network and any third-party network must be controlled and restricted on a business need basis.

11.5 Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities, in particular electronic messaging.

12.0 Systems Acquisition and Development Lifecycle

12.1 SEs must ensure that cybersecurity related requirements are considered when acquiring new information systems or enhancing existing information systems.

12.2 SEs must have in place effective controls to ensure that information (such as payments, internet banking or mobile banking apps) are protected from fraudulent activities, contract dispute and unauthorised disclosure and modification.

12.3 Rules for the development of software and system, including mandatory security requirements must be established by the SE, and applied to relevant developments within the entity. In this regard, secure system engineering principles, coding standards and programming techniques must be adopted by the SE and used in the system development process.

12.4 SEs must ensure that changes to systems within the development lifecycle are controlled by the use of formal change control procedures and the modifications to software packages are limited to necessary changes under a strict control environment.

12.5 SEs should establish and appropriately protect a secured development environment that covers the entire system development lifecycle. In addition, SEs should supervise and monitor outsourced system development activities.

12.6 During the system development phase, testing of security functionality should be carried out.

13.0 Third - Party Relations

13.1 The use of third-party services must not in any way result in any weakening of the cybersecurity control environment of the SE, or the assurance over its effectiveness.

13.2 SEs must develop and implement a third-party relationship policy that mandates cybersecurity controls to address the risk posed by third-party access to their information assets.

13.3 SEs must review the security policies, procedures and controls of third parties that have access to their information assets on a regular basis, including commissioning or obtaining periodic expert reports on the adequacy of the cybersecurity control environment and compliance to applicable regulation.

13.4 The third-party relationship policy must, at a minimum include:

a) appropriate due diligence processes for the appointment of third-party service providers, to determine its viability, reliability, and financial position;

b) limited third-party access with time limitations; and

c) management of changes to the provision of services by third parties taking into account the criticality of business information, systems and processes involved and reassessment of risks.

13.5 SEs must establish an effective service level agreement for any services provided by third parties that in any way requires or provides access to the SEs information assets. The service level agreement must include provisions in relation to cybersecurity that ensures the effectiveness of the SE's cybersecurity risk controls.

13.6 Third-party agreements must include clauses that reserves the right of the SE and the Reserve Bank to conduct reviews, including on-site examination of the activities, systems, sites, and facilities that are relevant to the provision of the contracted services.

14.0 Incident Management

14.1 SEs must have a cybersecurity incident management process governed by a documented policy, and procedures with the objective of restoring normal service as quickly as possible following an incident, and with minimal impact to business operations.

14.2 The cybersecurity incident management policy and procedures must at a minimum:

a) define what constitutes a cybersecurity incident and the criteria for incident categorisation, including criteria for categorising an incident as a crisis;

b) prioritise resolution based on defined severity levels;

c) address clear accountability and communication strategies to limit the impact of cybersecurity incidents ;

d) address evidence collection and preservation;

e) address the testing of the incident management process;

f) address employees' requirements to notify on incidents or indicators of possible incidents; and

h) clear and effective coordination with the Reserve Bank, Police and national cybersecurity organisations.

15.0 Security Audit and Testing

15.1 SEs are required to ensure that their approach to managing cybersecurity and its implementation, including the objectives, controls, policy, processes and procedure for cybersecurity, are reviewed independently at planned intervals or when significant changes occur.

15.2 SEs must ensure that an operationally independent and adequately resourced internal audit function covers the review of the CSRMF.

15.3 To ensure that cybersecurity is implemented and operated in accordance with the SE's policies and procedures, the following minimum security audit and testing requirements are to be observed:

a) conduct security audits and tests, including vulnerability scans and penetration tests, at regular intervals at a minimum for high risk systems and processes, and before such systems are introduced;

b) internal audit function to perform or commission security audits and tests at regular intervals according to their independent risk assessment; and

c) ensure that the internal audit function is sufficiently resourced, at a minimum to effectively assess the tests' planning, execution and reporting.

16.0 Cybersecurity Considerations of Business Continuity Management

16.1 Cybersecurity continuity must be embedded in the SE's business continuity management system and at a minimum should include the following requirements:

a) determine relevant requirements for cybersecurity and the continuity of cybersecurity risk management in adverse situations, e.g. during a crisis or disaster; and

b) establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for cybersecurity during an adverse situation.

17.0 Regulatory Reporting

17.1 Timely reporting of cybersecurity incidents is important in ensuring the protection of SEs and the financial system, at all times. SEs are required to report on cybersecurity incidents in the format prescribed as Appendix 2.

17.2 The SE must notify the Reserve Bank of Fiji within 24 hours[4] after becoming aware of a cybersecurity incident that materially affects or has the potential to materially affect financially or non-financially the institution, or the interests of depositors, policyholders, fund members, investors, or the general public who use the SE's services.

PART 3: OVERSIGHT AND IMPLEMENTATION ARRANGEMENTS

18.0 OVERSIGHT BY THE RESERVE BANK OF FIJI

18.1 Each SE must provide to the Reserve Bank a copy of its Cybersecurity policy and all relevant policies and procedures within 12 months of the implementation of this Policy. In the event of major changes made to the requirements of the Cybersecurity policy or policies relating to cybersecurity, copies of the revised policy must be submitted to the Reserve Bank within 30 days after the changes have been approved by the SE's board.

18.2 The Reserve Bank will assess compliance of each SE with the requirements of this Policy in the course of its supervision. A SE that fails to comply with

[4] The cyber incident reporting time stipulated in the policy differs from the operational risk incident reporting under BSPS No.16 Minimum Requirements for the Management of Operational Risk for Licenced Financial Institutions. SEs will continue to report both risk incidents.

the requirements of this policy will be subject to relevant sanctions by the Reserve Bank.

18.3 The Reserve Bank may adjust or exclude a specific requirement in this Policy by providing a written notice to the SE.

19.0 IMPLEMENTATION ARRANGEMENTS

19.1 This Policy becomes effective from 31 March 2023 with full compliance required within one year from the effective date.

Reserve Bank of Fiji
March 2023

Appendices

Schedule
Appendix 1 – Abbreviations List
Appendix 2 – Quarterly Report on Cybersecurity Risk Incidents

SCHEDULE

Interpretation –

(1) Any term or expression used in this Policy that is not defined in this Policy”

a) which is defined in the Banking Act 1995, Insurance Act 1998 ,Reserve Bank of Fiji Act (Cap.210), Reserve Bank of Fiji (Capital Markets and Securities Industry) Regulation 2015, Exchange Control Act 1985 and the Fiji National Provident Fund Act 2011.
unless the context otherwise requires, have the meaning given to it by the said Acts; and,

b) which is not defined in the Acts and which is defined in any of the Reserve Bank of Fiji Policy Statements shall, unless the context otherwise requires, have the meaning given to it by those policy statements.

(2) In this Notice, unless the context otherwise requires:

‘Act’ means the Banking Act 1995, Insurance Act 1998, Reserve Bank of Fiji Act (Cap 210), Reserve Bank of Fiji (Capital Markets and Securities Industry) Regulation 2015, Exchange Control Act 1985 and the Fiji National Provident Fund Act 2011.

‘Board’ means the board of the SE.

‘Availability’ means timely and reliable access to, and use of information.

‘Confidentiality’ means access being restricted only to those individuals, entities or processes authorised.

‘Criticality’ means the degree of importance to potential loss of availability.

‘Cryptography’ means the science of protecting information by transforming it into a secure format

‘Cybersecurity’ means controls and processes to preserve the confidentiality, integrity and availability of information assets.

‘Cybersecurity Capability’ means the totality of resources, skills and controls which provide the ability and capacity to maintain information security.

‘Cybersecurity Control’ means a prevention, detection or response measure to reduce the likelihood or impact of an information security incident.

‘Cybersecurity Incident’ means an actual or potential compromise of the confidentiality, integrity or availability of an institution’s system or data.

‘Cybersecurity Policy Framework’ means the totality of policies, standards, guidelines and procedures pertaining to information security.

‘Cybersecurity Threat’ means a circumstance or event that has the potential to expose an information security vulnerability.

‘Information System’ means a set of applications, services, **information** technology assets or other **information**-handling components, which includes the operating environment.

‘Information Asset’ means information and information technology, including software, hardware and data (both soft and hard copy).

‘Integrity’ means completeness, accuracy and freedom from unauthorised change or usage.

‘Malware’ means a collective term used to describe a variety of malicious programs (including viruses, worms, Trojan horses, ransomware, spyware, adware, shareware etc.) designed to spread and replicate from computer to computer through communication links or through sharing of electronic files to interfere with or damage computer operation.

‘Sensitivity’ means the potential impact of a loss of confidentiality or integrity

‘Software System End of Life’ means with respect to a software product, indicating that the product is at the end of its useful life.

‘Third Party’ means any supplier of information systems services

Appendix 1

List of Abbreviations and Acronyms

BCM	Business Continuity Management
BIS	Bank of International Settlements
CISO	Chief Information Security Officer
CSRMF	Cybersecurity Risk Management Framework
CSS	Cybersecurity Strategy
ICT	Information and Communication Technologies
IMF	International Monetary Fund
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
QCR	Quarterly Condition Report
RBF	Reserve Bank of Fiji
SEs	Supervised Entities
SE	Supervised Entity
WLAN	Wireless Local Area Networks

Appendix 2

Form QCR Quarterly Report on Cybersecurity Risk Incidents

Reporting Institution Name:				**Reporting Quarter:**	
Cyber security root cause Areas	**Event Number**	**Incident Number**	**Value of Loss**	**No. Unresolved from prior period**	**No. Resolved Current Quarter**
Asset Management					
Access Controls					
Operations Security					
Communication Security					
System Acquisition, Development & Maintenance					
Third Party relationships					
Security Audit and Testing					
Information Sec. BCM					
Human Resource					
Cryptography					
Physical & Environmental					
Other					
Total					