[XX 2019]

Rule
Cybersecurity for Regulated Entities

1. Statement of Objectives

1.1. To set out the Cayman Islands Monetary Authority's ("the Authority") Rule on cybersecurity applicable to regulated entities, (each of the sub-paragraphs of section 5 below referred to as a "Rule," and collectively, the "Rules"), pursuant to the Monetary Authority Law ("MAL").

1.2. The Authority acknowledges that technology presents important innovation, competitive advantages as well as greater efficiency, effectiveness and productivity for regulated entities and their clients. However, a significant compromise in the use of technology could impact the ability of regulated entities to meet overall business objectives or result in significant liability and reputational damage. Therefore, it is important for regulated entities to ensure that robust cybersecurity measures are in place and that they can appropriately identify, protect, detect, respond to and recover from such cybersecurity-related threats, incidents and breaches.

2. Statutory Authority

2.1. Section 34 of the MAL provides that:

> *(1) After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may -*
>
> *(a) issue or amend rules or statements of principle or guidance concerning the conduct of licensees and their officers and employees, and any other persons to whom and to the extent that the regulatory laws may apply;*

2.2. This document establishes the Rule on cybersecurity for regulated entities and should be read in conjunction, where applicable, with the:

(a) Statement of Guidance on Cybersecurity
(b) Rule and Statement of Guidance on Internal Controls
(c) Rule on Risk Management for Insurers
(d) Rule on Corporate Governance for Insurers (Insurance)
(e) Statement of Guidance on Corporate Governance
(f) Statement of Guidance on Operational Risk (Banking)
(g) Statement of Guidance Business Continuity Management
(h) Statement of Guidance on Outsourcing
(i) Statement of Guidance on the Nature, Accessibility and Retention of Records

2.3. This document should also be read in conjunction with other regulatory instruments issued by the Authority from time to time.

3. Scope of Application

3.1. This Rule applies to entities regulated by the Authority including controlled subsidiaries as defined in the Banks and Trust Companies Law. For the purpose of this Rule, a regulated entity is an entity that is regulated under the:

(a) Banks and Trust Companies Law
(b) Insurance Law
(c) Mutual Funds Law[1]
(d) Securities Investment Business Law
(e) Building Societies Law
(f) Cooperative Societies Law
(g) Development Bank Law
(h) Money Services Law
(i) Companies Management Law
(j) Directors Registration and Licensing Law
(k) Private Trust Companies Regulations

3.2. Regulated entities that are natural persons must ensure that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients' data or the regulated entities' systems, where applicable. The Rule on cybersecurity along with the corresponding Guidance on cybersecurity should be considered and applied, where applicable to ensure that there is a suitably robust cybersecurity framework in place.

3.3. Regulated entities such as Class 'B', 'C' and 'D' insurers that are fully managed by a licensed insurance manager are only required to comply with Rule 5.4. Insurance Managers must ensure that the cybersecurity framework implemented in respect of insurers that they manage is appropriate for the size, nature and complexity of the said insurers and meets their specific needs and risk tolerance.

3.4. Private Trust Companies, as registrants, must consider their cybersecurity risk, their risk tolerance and implement a framework appropriate to meet their cybersecurity needs.

[1] **Exceptions:** Regulated mutual funds.

4. Definitions

4.1. The following definitions are provided for the purpose of this Rule:

a) **Cybersecurity breach:** A penetration of the defences established to protect against cyber-risk.

b) **Cyber-attack**: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

c) **Cyber-risk:** the risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system. **Cyber-resilience:** the ability of systems and organizations to develop and execute long-term strategy to withstand cybersecurity events; practically, it is measured by the combination of mean time to failure and mean time to recovery.

d) **Cyber-space:** A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

e) **Cybersecurity:** an approach or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of and, as needed, to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems. **Cybersecurity Framework:** A complete set of organizational resources including policies, staff, processes, practices and technologies used to assess and mitigate cyber-risks and attacks.

f) **Cybersecurity incident:** A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

g) **Cybersecurity threat:** An event or condition that occurs that might exploit a vulnerability to breach defences that were established to protect against cyber-risk.

h) **Governing body:** in the case of a company, the Board of Directors and in the case of partnerships, the general partners. In the case of a branch or of an entity incorporated or established outside of the Cayman Islands, a management committee or body (beyond local management) empowered with oversight and supervision responsibilities for the entity in the Cayman Islands.

i) **Information technology ("IT"):** means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

j) **Information technology risk:** IT risk is the risk of mission or business loss resulting from particular threat source exploiting, or triggering, a particular information technology vulnerability.

k) **Information system**: means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

l) **Risk Management:** The use of structures, processes and people that identify, assess, mitigate and monitor all internal and external sources of risk that could have a material impact on operations.

m) **Recover Point Objective:** The point in time to which data must be recovered after an outage.

n) **Recover Time Objective:** definition: The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.

5. Rules

5.1. The Cybersecurity Framework

a) Regulated entities must establish, implement, and maintain a

documented cybersecurity framework that is capable of promptly identifying, measuring, assessing, reporting, monitoring and controlling or minimising cybersecurity risks as well as responding to and recovering from cybersecurity breaches that could have a material impact on their operations.

b) The cybersecurity framework of regulated entities must include, but is not be limited to:

i. a well-documented cybersecurity risk management strategy, approved by the Governing body, which addresses all material cybersecurity risks to which the regulated entities are likely to be exposed based on their business activities and use of technology;

ii. cybersecurity and IT security policies and procedures that are adequate to identify, assess, mitigate, control, monitor and report on such risks to which regulated entities are exposed;

iii. clearly identified managerial responsibilities and controls, designed to ensure that the policies and procedures established for cybersecurity and risk management are always adhered to; and

iv. clear and effective processes for containing and recovering from cyber-attacks and incidents as quickly as possible or within regulated entities' Governing body approved Recover Point Objective or Recovery Time Objective depending on the type of attack or incident.

c) Regulated entities must regularly review the cybersecurity arena and information technology space and assess their cybersecurity framework to ensure that the framework continues to be appropriate to manage adverse impacts of the cyber-risks and IT risks related to the regulated entities' business.

5.2. **Role of the Governing Body**

a) Regulated entities' Governing bodies are ultimately responsible for cybersecurity and the bodies' duties must include, but not be limited to:

i. approval of a written cybersecurity risk management strategy aligned with the overall business strategy and risk tolerance as well as approval of completed cybersecurity risk assessments and cybersecurity risk management as part of regulated entities' overall risk management strategies and programs;

ii. approval of a comprehensive cybersecurity framework;

iii. appropriate oversight of the risk management framework to ensure that policies and processes are implemented effectively;

iv. periodic review of the cybersecurity framework; and

v. approval of the cybersecurity audit plan and ensuring that any findings are addressed in a timely manner.

5.3. **Group and related entities**

a) The Authority recognizes that some regulated entities' risk management forms part of their parent company's risk management function. In these cases, the Authority does not expect them to duplicate functions that are already carried out by the parent. However, they should assess and document that an appropriate cybersecurity framework is in place on a group wide basis and at the legal entity level.

b) The Group cybersecurity framework must, at a minimum, cover the requirements noted in this Rule.

5.4. **Managed Entities**

a) The Authority recognises that certain regulated entities are fully managed by a licensed service provider. Furthermore, these entities might not develop their own cybersecurity framework but rather rely on the framework of their service provider. Such regulated entities that are managed by entities licensed by the Authority must make appropriate enquiries, through their Governing body, to satisfy themselves with the level of cybersecurity applied by that manager.

b) Regulated entities, as referred to in 5.4(a),

i. are ultimately responsible for their cybersecurity and for assessing the service provider(s)' compliance with this Rule and related guidance on cybersecurity; and

ii. must satisfy themselves that the cybersecurity framework that will be applied in respect of the services provided to them is appropriate for the cybersecurity risks posed to them as a result of the use of technology and emerging cybersecurity threats.

c) The Governing body of a regulated entity referred to in 5.4(a) must require the service provider to report any cybersecurity related breaches that pertain to the regulated entity. A mechanism must be in place to ensure that the regulated entities are aware through the Governing body what services are being provided to them by their insurance managers.

5.5. **Cybersecurity Awareness, Training, Awareness and Resources**

a) Regulated entities must establish a comprehensive training and awareness program[2] relating to cybersecurity and cyber-resilience that is endorsed by the Governing body and/or senior management. It should be reviewed and updated to ensure that the contents of the program remain current and relevant by taking into consideration the evolving nature of technology as well as emerging risks including risk areas for the regulated entity.

5.6. **Management of Outsourcing Risks**

a) Regulated entities that outsource information technology functions either externally to third parties or internally to affiliated entities;

i. remain ultimately responsible for outsourced IT functions and their cybersecurity;

ii. must ensure that they assess the service provider(s)' compliance with this Rule and related guidance on cybersecurity and outsourcing; and

iii. must have oversight and clear accountability for all outsourced functions as if these functions were performed by the regulated entities themselves and subject to the normal standards of their cybersecurity and IT security framework.

b) Regulated entities should consider outsourcing arrangements that go beyond IT-related functions that may also present a cybersecurity risk.

6. Data Protection

6.1. Regulated entities must demonstrate that data protection is part of their strategy and cybersecurity framework.

7. Notification Requirements

7.1. Regulated entities must immediately notify the Authority in writing of an incident when it is deemed to have a material impact or has the potential to become a material incident and no later than 72 hours following the discovery of said incident.

7.2. Regulated entities should define incident criticality in their incident management framework. When in doubt about the level of seriousness of an event, regulated entities should consult the Authority. Reportable incidents may fall into one or more of the following:

[2] Training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. (Source: NIST Special Publication 800-16)

a) Material impact to the regulated entity's internal operations.
b) The event results in the unauthorized dissemination of ANY personal data either internally or externally.
c) Significant operational impact to internal users that is material to customers or business operations.
d) Extended disruptions to critical business systems or internal operations;
e) Number of external customers impacted is significant or growing.
f) If determined that there is potential reputational impact, either to the entity or the Cayman Islands, notification to the Authority must occur immediately if there is any risk of premature public disclosure.
g) Any loss of any card payment information, beneficial owner details, or any personally identifiable information.
h) Loss or exposure of any data in violation of any applicable data protection laws both foreign and domestic.

7.3. For regulated entities that have risk ratings in respect of their cyber-risks, the Authority expects that the required notification includes ratings that correspond to a material incident.

7.4. Regulated entities must notify affected persons if a cyber-attack results in the breach of non-public information or disrupts a service that is utilised including information on the action taken to contain (as necessary), remedy and recover from the breach.

8. Enforcement

8.1. Whenever there has been a breach of the Rules, the Authority's policies and procedures as contained in its Enforcement Manual will apply, in addition to any other powers provided in the regulatory laws and the MAL.

9. Effective Date

9.1. This Rule will come into effect within six months of the date that it is published in the Gazette.