RULE

Cybersecurity for Regulated Entities

April 2023

List of Acronyms

IT	Information Technology
MAA	Monetary Authority Act
SOG	Statement of Guidance

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, pursuant to the Monetary Authority Act ("MAA").

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(1)(a) of the MAA provides that:

After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may -

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, with other regulatory instruments issued by the Authority from time to time, where applicable.

3. Scope of Application

3.1 This Rule applies to entities regulated by the Authority[1] including controlled subsidiaries as defined in the Banks and Trust Companies Act (as amended). For the purpose of this Rule, a regulated entity is an entity that is regulated by the Authority in accordance with the regulatory Acts, as defined in the MAA (as amended).

3.2 References to any act or regulation shall be construed as references to those

[1] Exceptions are a) Regulated Mutual Funds as defined in the Mutual Funds Act (as amended); and b) Private Funds as defined in the Private Funds Act (as amended).

provisions as amended, modified, re-enacted, or replaced from time to time.

3.3 Regulated entities 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. Regulated entities should apply this Rule and consider the corresponding *Statement of Guidance ("SOG") – Cybersecurity for Regulated Entities*, where applicable, to ensure that there is a suitable and robust cybersecurity framework in place.

3.4 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 6.3. Insurance Managers must ensure that the cybersecurity framework implemented in respect of insurers that they manage is commensurate with the size, complexity, structure, nature of business and risk profile of the operations of the said insurers and meets their specific needs and risk tolerance.

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

4. Definitions

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

4.1.1 **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.

4.1.2 **Cyber resilience:** The ability of systems and organisations 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.

4.1.3 **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 unauthorised access, use, disclosure, disruption, modification, or destruction of the manufacturing system.

4.1.4 **Cybersecurity:** An approach or series of steps to prevent or manage the risk of damage to, unauthorised 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.

4.1.5 **Cybersecurity breach:** Any unauthorised penetration of the defences[2]

[2] Defences may be internal or external.

established to protect against cyber risk.

4.1.6 **Cybersecurity framework:** A complete set of organisational resources including policies, staff, processes, practices and technologies used to assess and mitigate cyber risks; and respond to and recover from cyber attacks.

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

4.1.8 **Cybersecurity threat:** Any circumstance or event with the potential to adversely impact organisational operations, organisational assets, individuals, other organisations, or the country through a system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.

4.1.9 **Cyberspace:** 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.

4.1.10 **Governing body:** the Board of Directors where the entity is a corporation, the General Partner where the entity is a partnership, the manager (or equivalent) where the entity is a Limited Liability Company, and the Board of Trustees where the entity is a trust business.

4.1.11 **Information technology ("IT"):** 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.

4.1.12 **Information technology risk:** The risk of mission or business loss resulting from a particular threat source exploiting, or triggering, a particular information technology vulnerability.

4.1.13 **Information system**: 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 specialised system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

4.1.14 **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.

4.1.15 **Risk tolerance:** An entity's readiness to bear the risk after risk treatment in order to achieve its objectives.

4.1.16 **Recovery Point Objective:** The point in time to which data must be recovered after an outage.

4.1.17 **Recovery Time Objective:** 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

5.1.1 Regulated entities must establish, implement, and maintain a documented cybersecurity framework that is designed to promptly identify, measure, assess, report, monitor and control or minimise cybersecurity risks as well as responding to and recovering from cybersecurity breaches that could have a material impact on their operations.

5.1.2 The cybersecurity framework of regulated entities must include, but is not be limited to the following:

a) 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;

b) 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;

c) 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

d) clear, documented, and effective processes for responding to, containing, and recovering from cyber attacks, cybersecurity breaches and incidents as quickly as possible or within regulated entities' governing body's approved Recover Point Objective or Recovery Time Objective depending on the type of attack or incident.

5.1.3 Regulated entities must regularly review the emerging (or evolving) cybersecurity threats and IT landscape 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.

6. Role of the Governing Body

6.1 Regulated entities' governing bodies are ultimately responsible for cybersecurity and their duties must include, but not be limited to:

a) 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 programmes;

b) approval of a comprehensive cybersecurity framework;

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

d) periodic review of the cybersecurity framework; and

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

6.2 **Group and related entities**

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

6.2.2 The cybersecurity framework should be implemented on a consolidated basis and must at a minimum cover the requirements noted in this Rule.

6.3 **Managed Entities**

6.3.1 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 service provider.

6.3.2 Regulated entities, as referred to in 6.3.1:

a) are ultimately responsible for their cybersecurity and for assessing the service provider(s)' compliance with this Rule and the related SOG on Cybersecurity for Regulated Entities; and

b) 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.

6.3.3 The governing body of a regulated entity referred to in 6.3.1 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.

6.4 Cybersecurity Awareness, Training and Resources

6.4.1 Regulated entities must establish a comprehensive training and awareness programme[3] relating to cybersecurity and cyber-resilience that is endorsed by its governing body and/or senior management. It should be reviewed and updated to ensure that the contents of the programme 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.

6.4.2 Regulated entities must ensure that they have sufficient and suitable personnel to maintain their cybersecurity framework, commensurate with the size, complexity, structure, nature of business and risk profile of its operations.

6.5 Management of Outsourcing Risks

6.5.1 Regulated entities that outsource IT functions either externally to third parties or internally to affiliated entities:

a) remain ultimately responsible for outsourced IT functions and their cybersecurity;

b) must ensure that they assess the service provider(s)' compliance with this Rule and related SOG on Cybersecurity for Regulated Entities and the SOG - Outsourcing: Regulated Entities; and

[3] 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)

c) 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.

6.5.2 Regulated entities should also make considerations for outsourcing arrangements that go beyond IT-related functions that may also present a cybersecurity risk.

7. Data Protection

7.1 Regulated entities must demonstrate that data protection is part of their strategy and cybersecurity framework taking into consideration the provisions of the Data Protection Act and the guidance issued by the Cayman Islands Ombudsman on data protection.

8. Notification Requirements

8.1 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.

8.2 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. Incidents should be reported to the Authority if they fall under one or more of the following:

a) Material impact to the regulated entity's internal operations.

b) The event results in the unauthorised 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 regulated entity or the Cayman Islands as a whole, 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 Acts and other regulatory requirements both foreign and domestic.

8.3 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.

8.4 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.

9. Enforcement

9.1 Whenever a breach of these Rules occurs, the Authority's policies and procedures, as contained in its Enforcement Manual, will apply, in addition to any other powers provided in the regulatory Acts and the MAA.

SIX, Cricket Square
PO Box 10052
Grand Cayman KY1 - 1001
CAYMAN ISLANDS

General Office: 345-949-7089

www.cima.ky