Guernsey Financial Services Commission

# Cyber Security Rules and Guidance 2021

Issued 5th February 2021

**CONTENTS**

## Introduction

Technology risks including information security, cyber security and data privacy are all key considerations for licensed firms and persons ("Firms") regulated by the Guernsey Financial Services Commission ("the Commission") and should be considered by other interested parties.

The Commission applies a pragmatic, risk-based approach, to regulating the Bailiwick's financial services sector and this is reflected in the Cyber Security Rules, 2020 ("the Rules").

As with other material risks, all licensed institutions are required to have robust policies, procedures and controls in place to identify, assess and manage cyber security risks on an on-going basis consistent with the minimum licensing requirements.

These Rules focus on five core principles outlined in a number of international cyber security frameworks –

- Identify, Protect, Detect, Respond and Recover.

The Commission recognises that there is no "one size fits all" approach to addressing cyber risks with specific business circumstances varying greatly from Firm to Firm. It may be appropriate for Firms to consider accreditation or certification from a recognised body, such as Cyber Essentials[1], Cyber Essentials Plus or ISO270001. These accreditations may help a Firm in meeting some of the requirements set out in the Rules, however, accreditation alone is unlikely to result in full compliance.

The following guidance provides Boards[2] with examples of how a Firm may satisfy the requirements laid out in the Rules. Not all of the examples outlined in this guidance will be relevant to all Firms and it remains the responsibility of the Board to ensure that the Firm complies with the Rules.

Firms that outsource large portions of their operation are still expected to comply with the Rules, however it may be reasonable for the Board of such an entity to expect the outsourced provider to complete much of the control framework outlined in the Rules and this guidance. The Board would, nonetheless, be expected to have oversight of these services and would be responsible for compliance with these Rules.

This guidance may also be used by non-licensed firms such as Prescribed Businesses or Non-Regulated Financial Services Business.

[1] Cyber Essentials and Cyber Essentials Plus are NCSC backed schemes that attempt to protect organisations against Cyber Risks www.ncsc.gov.uk/cyberessentials/overview.

[2] Throughout this guidance the term 'Boards' is used to refer to any group or individual who would hold a comparative position, to the Board, in a Firm.

In addition to the below Guidance the Commission recommends that Firms consider the resources made available on the UK Government National Cyber Security Centre website www.ncsc.gov.uk.

The Cyber Security Rules, 2021 are set out in red text boxes.

## Application and Operation

### 1.1 Application and operation

(1) These Rules have direct application to all licensees who are licensed under the Regulatory Laws.

(2) The Board of Directors of the licensee, or equivalent, is responsible for ensuring that these Rules are followed.

(3) All licensees must be able to provide evidence, to the Commission on request, that these Rules have been considered and implemented in accordance with the size, nature and complexity of the licensee's business.

(4) The licensee must, taking into consideration the size, nature and complexity of its business, have in place appropriate policies, procedures and controls to mitigate the risk posed by cyber security events. Any policies, procedures and controls adopted, by the licensee, must reflect these Rules and take into consideration any guidance issued by the Commission.

(5) All relevant measures adopted, by the licensee in order to comply with these Rules, must be reviewed –

- (a) in response to a trigger event;
- (b) following an identified cyber security event; or
- (c) at least periodically

and must be recorded by the licensee.

(6) The Commission may in its absolute discretion, by written notice to a licensee, exclude or modify the application of any provision of these Rules if the licensee satisfies the Commission that such a derogation does not prejudice the interests of the clients of the licensee or the reputation of the Bailiwick.

**Periodic Review**

Depending on the size, nature and complexity of a Firm, the Board should decide on the frequency of periodic reviews. The Commission would not expect periodic reviews to take place any less frequently than every 24 months and Boards should report to their shareholders that they are comfortable with their Cyber policies, controls and reporting on an annual basis.

## Identification of Assets and Risks

**2.1 Risk Assessment of Cyber Vulnerabilities and Risk**

(1) The licensee must ensure that it has taken appropriate steps to identify all of its material assets and carried out an assessment of significant associated cyber risks.

### Assets and Data

A Firm should ensure it is able to identify the assets and data it holds and assess the damage, to its business, if it lost access to those assets or if the data it holds were to suffer a breach of confidentiality, integrity or availability. These assets should not be limited to traditional IT assets and should include systems, people and data assets.

When considering the requirement to identify assets, in line with rule 2.1, Firms should consider the materiality and the possible underlying risks associated with that asset. All assets should be considered through a cyber security lens but not all assets will require bespoke or in depth analysis.

Without knowing what you have to protect you cannot determine the appropriate controls to protect it. This assessment of cyber risks could be a standalone document or could be part of a pre-existing risk assessment document.

The Commission recognises that a Firm may hold assets using cloud services or similar outsourced service. It is the expectation that a Firm would identify these assets held in this manner in the same way they would any other outsourced provider.

### Risks

The Commission expects that the Board of all licensed Firms, or the relevant board committee, will have evaluated the Cyber Risks associated with the assets that it has identified and reviewed the impact that a cyber security event would have on the integrity, availability and confidentiality of those assets. Understanding the risks associated with the assets held will enable Firms to judge the appropriate level of controls and mitigants that are needed.

## Protection and Detection

**3.1 Protecting IT Services**

(1) The licensee must ensure that it has the appropriate policies and controls in place to mitigate the risks it has identified and to ensure, where possible, the delivery of critical infrastructure during and following a cyber security event. These policies and controls should include but are not limited to –

(a) having appropriate cyber security software in place;

(b) ensuring that IT system updates, from infrastructure and software providers, are implemented in a timely manner;

(c) the provision of employee training to enable the recognition of possible cyber security events;

(d) having policies in place to ensure that all users are aware of their impact on cyber security.

**4.1 Detecting Cyber Security events**

(1) The licensee must have appropriate mechanisms in place in order to identify the occurrence of a cyber security event.

### Policy and Controls

Following the identification and evaluation of cyber risks, Firms are expected to put in place processes, procedures and controls that are appropriate for the size, nature and complexity of their businesses and the risks faced. These controls and policies should be used to fulfil the Protect and Detect principles outlined in the Rules including the requirement to continue to deliver critical infrastructure where possible.

The Commission recognises that a Firm's ability to identify cyber security events may not be effective 100% of the time. A Firm should document how it has assessed the appropriateness of these controls, and its approach to mitigation, for the size and complexity of its business.

Controls can broadly be categorised under the following headings:

1- Technical Controls
2- People Controls
3- Administrative Policy and Governance Controls.

**1. Technical Controls**

Technical Controls are procedures and controls that result in security measures executed or controlled through computer systems. They offer automated protection against misuse, unauthorised access to valuable information, facilitate security violation detection and support requirements of security related to data and application.

The variety of Technical Controls available is vast and not all Technical Controls will be suitable to all Firms. Each Firm should consider which controls are suitable to their circumstances and should document these decisions. Technical Controls include, but are not limited to -

*Network monitoring tools*

Network monitoring tools enable Firms to monitor their networks and to detect security related events. Early identification of events can result in reducing damage and disruption.

*Vulnerability management.*

Vulnerability Management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. Vulnerability management tools can include scheduled penetration tests and the use of automated system scanning tools.

*Patch Management*

Patch management is the process that helps acquire, test and install patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated.

All security patches should be reviewed not just those that are flagged as critical or high. Lower rated vulnerabilities are used in vast numbers of attacks partly because some Firms don't prioritise patching them so remain exposed for longer.

*2 Factor Authentication (2FA)/Multi Factor Authentication (MFA)*

Firms should consider activating 2FA or MFA on any account accessed over the internet. 2FA or MFA adds an extra layer of security to every online platform accessed. The first layer is generally a combination of a username and password. The second layer is a further requirement to authenticate your identity; traditionally a code or token that has been sent to your email or generated by an application on a device. Adding the additional layer in the process to authenticate your identity makes it harder for an attacker to access your data.

2FA/MFA is a simple and cost effective measure to increase security of access to online systems.

*Email protection tools (phishing)*

Successful phishing attacks are one of the most common causes of cyber security breaches. The risks from phishing are extremely difficult to completely mitigate using technical controls. However, Firms can benefit from a technical solution in filtering out a lot of phishing emails, spam, spear-phishing and other email based threats and should consider the appropriateness of these tools.

Firms should consider how they can increase employee awareness of phishing threats.

*Antimalware*

Antivirus or antimalware controls are universally used, however, older or less comprehensive antivirus solutions can depend on outdated signature based rules that are susceptible to more modern malware or viruses. Antivirus or antimalware programmes should be reviewed regularly to ensure they are fit for purpose and able to detect newer threats and configuration settings reviewed to ensure that the antivirus or antimalware programmes are delivering the expected level of protection.

*Mobile Device Management*

Firms should give consideration to the appropriateness of employing mobile device management (MDM) solutions to ensure that corporate data is suitably secure.

*Data Loss Prevention tools*

Firms should consider the appropriateness of data loss prevention tools that enable them to gain visibility of data loss and ultimately provide better detection and prevention of the unauthorised exfiltration of sensitive or confidential corporate data.

*Encryption*

Firms should consider the appropriateness of encrypting their data at rest or in transit, including on removable storage and mobile devices or when data is sent across an untrusted network.

## 2. People Controls

Users have a critical role to play in their Firm's security and so it is important that policies and procedure, and the technology provided, enable users to do their job as well as keeping the Firm secure. This can be supported by a systematic delivery of awareness programmes and training, that delivers security expertise, as well helping to establish a security-conscious culture.

*User/staff training*

Human error is one of the biggest threats to the cyber security of a Firm.

All new joiners to the organisation should be clear on the cyber security culture and cyber security training should be mandatory for every new employee.

Training programmes should be formalised and should be updated and repeated regularly; making cyber training a continuous process.

Best practice for a security awareness training programme should include, without limitation -

- Email Scams, Phishing and Social Engineering;
- Passwords;
- Clear Desk Policy;
- Bring-Your-Own-Device ("BYOD") Policy (if the Firm allows the use of personal devices);
- Data Management;
- Removable Media;
- Safe Internet Habits;
- Physical Security and Environmental Controls;
- Social Networking Dangers;
- Malware;
- Hoaxes.

*Phishing Testing*

Formalised and structured phishing testing should be carried out on a regular basis. Simulating phishing attacks enables a Firm to assess its cyber maturity and security

awareness, as well as that of its staff, and aids the development of effective phishing awareness training initiatives.

## 3. Administrative Policy and Governance Controls

It is important for every Firm to have documented security policies to help protect the Firm's data and other assets. Documented security policies that clearly define a Firm's position on security can be of critical importance in the event of a security incident or data breach.

### *Creation and maintenance of policies and procedures*

The three core objectives for information security policies should be -

- Confidentiality – the protection of IT assets and data from unauthorised users;
- Integrity – ensuring that IT assets and data are correct, accurate, able to be relied upon and have not been changed or modified in an unauthorised manner;
- Availability – ensuring IT assets, data and networks are available to authorised users.

Firms should, at a minimum, consider the following areas when compiling policies and procedures: -

- Acceptable Use Policy;
- Confidential Data Policy;
- Email Policy;
- Mobile Device Policy;
- Network Security Policy;
- Password Policy;
- Physical Security Policy;
- Wireless Network and Guest Access Policy;
- Access Management Policy.

These policies could exist as separate documents or in one single document.

### *Review of existing tools, products and services*

A Firm should conduct regular reviews of the security tools, products and services that it has in place to ensure that they are -

- fit for purpose;
- being utilised to the fullest extent possible/applicable;
- configured to the bespoke needs of the Firm;
- adequate enough to meet existing and near future needs;
- providing appropriate protections for the risks the Firm faces.

*Management Information*

Firms should ensure that reporting to the Board, or the relevant board committee, on cyber matters is fit for purpose and contains adequate information to inform the Board and allow it to make decisions and direct attention where it is needed.

Where appropriate Firms should have the capability to monitor their networks and to detect and record security related events. Meaningful data should be supplied to the Board. Management Information ("MI") should go beyond what is happening at the perimeter of the network and should include what is going on inside the network and what the Firm is doing to defend itself.

Relevant MI will differ for each Firm based on its size, nature and complexity. The Commission does not require a Firm to provide a mandated list of MI to its Board but expects a Firm to consider the MI that is relevant to its unique position. A Firm may wish, but is not mandated, to consider providing the following MI -

### Current Cyber Security Risks

- Patching/vulnerability status – details of vulnerabilities not patched across the estate, aged by criticality, i.e. criticals/highs/mediums/lows unpatched over 30, 60, 90, 180, 365 days, etc., with reasons why patches have not been applied or detail of mitigating controls that exist;
- List any unsupported operating systems/software, roadmaps to migrate to supported versions or timeline to decommission;
- Staff education and awareness updates - how many staff are still to complete mandatory annual security training;
- Phishing simulation click rates;
- Findings of the most recent penetration test and when findings will be mitigated;
- Third Party Management.

### Emerging Risks, Threats and Vulnerabilities

- What is happening in terms of emerging risks, threats and vulnerabilities; top stories from open source or other threat intelligence feeds; etc.

### Incidents

- Numbers of actual events (with analysis on why; did tools work/not work; whether this is a wider risk; what actions are required; lessons learned; etc.);
- Significant near miss events;
- Actual breaches;

- Data loss events;
- Phishing attacks blocked.

### Compliance Status

- How compliant is the Firm with any regulatory requirements, standards and any models or accreditations with which it is aligned, either locally or as part of a group entity.

## **Materiality**

When a Firm reviews or implements cyber controls, policies and procedures it should consider whether these are appropriate for its business and whether they are already covered by existing control frameworks.

## Respond and Recover

**5.1 Responding to Cyber Security events**

(1) The licensee must be able to demonstrate that it has a plan in place which aims to mitigate any disruption caused by a cyber security event.

(2) Where the licensee is part of a group and the maintenance and recovery of IT systems is controlled at group level; the licensee must be able to demonstrate that it is aware of any group plan specific to the systems it uses and that the plan is appropriate to the licensee.

(3) Where the maintenance and recovery of the licensee's IT systems are outsourced to a third party provider it must ensure that it is aware of any plan which has been put in place, by that provider, and that the plan is appropriate to the licensee.

**6.1 Recovery from a Cyber Security event**

(1) The licensee must be able to demonstrate that it is aware of the appropriate steps that need to be taken in order to restore business capabilities, following a cyber security event, and ensure essential activities are capable of being undertaken in the interim period.

In the event of a cyber security event occurring Firms are expected to have processes, procedures and controls in place that allow them to assess the impact of the event and to respond and recover as described in the Respond and Recover sections of the Rules. The Commission recognises that it is not practical to expect a Firm to be able to predict all possible disruption that an unknown cyber security event may cause, however it does expect Firms to be able to evidence that they have considered what scenarios are relevant for their business.

The sophistication of these processes, procedures and controls should be appropriate for the size, nature and complexity of its business. Firms should consider the following controls -

## Technical Controls

*Backups*

A Firm should ensure it has adequate backups both online and, where appropriate, offline or unconnected to a Firm's main network. Online backups should be connected to systems, and be backed up in real time or at a frequency agreed in the Firm's relevant policies and procedures. Offline, or unconnected, backups should not be connected to the network so that they cannot be themselves corrupted in the event of ransomware.

A Firm should ensure it tests restoring from backups and that the backups provide the expected restored data.

## Policy and Governance Controls

*Incident Response Planning and Exercising around a Cyber Security Event*

Firms should have a documented incident response plan in place; outlining the actions that should be undertaken in the event of a cyber security event. This plan should be well known to key stakeholders and should be rehearsed on a periodic basis.

*Recovery Planning following a Cyber Security Event*

Firms should have a recovery plan in place. Effective planning is a critical component of a Firm's preparedness for cyber security event recovery. Recovery planning enables Firms to understand system dependencies; critical personnel identities such as crisis management and incident management roles; arrangements for alternate communication channels, services, and facilities; and many other elements of business continuity.

Planning also enables Firms to explore "what if" scenarios, which might be largely based on recent cyber security events that have negatively impacted other organisations, in order to develop customised playbooks. Thinking about scenarios helps the Firm to evaluate the potential impact, planned response activities, and resulting recovery processes long before an actual cyber security event takes place. These exercises help identify gaps that can be addressed before a crisis situation, reducing their business impact. Such scenarios also help to exercise both technical and non-technical aspects of recovery such as personnel considerations, legal concerns, and facility issues.

Both incident response and recovery plans could be considered as standalone documents or could be included as part of a Firm's business continuity and disaster recovery plans.

## Notification

**7.1. Notification to the Commission**

(1) A licensee must notify the Commission, as soon as reasonably practicable, upon becoming aware of a cyber security event which has resulted in –

(a) any loss of significant user data;

(b) significant loss of availability to IT systems;

(c) significant cost to the business;

(d) significant loss of business capability;

(e) significant loss of service to users.

(2) The notification must include the following details pertaining to the cyber security event –

(a) date on which it was discovered;

(b) date on which it occurred;

(c) its nature;

(d) current resulting consequences;

(e) any possible future consequences;

(f) actions taken to mitigate the consequences;

(g) any further steps to be taken.

## Notification Requirements

The notification requirements under the Rules are not intended to replace any separate notification requirements a Firm may have

## General Provision

**8.1. Interpretation**

(1) In these Rules terms have their ordinary meaning unless specifically defined.

(2) In these Rules the following definitions should be followed -

**"cyber security event"** means any occurrence which threatens, or has the potential to threaten, the confidentiality, integrity or availability of any IT Assets or services utilised by the licensee in the course of its business;

**"critical infrastructure"** means any system or service, utilised by the licensee in the course of its business, the loss of confidentiality, integrity or availability of which would lead to the failure of the operations of the licensee;

**"trigger event"** means any significant occurrence which would indicate that the licensee may be susceptible to a cyber security event. Such occurrences, dependent on severity, may include, but are not limited to –

(a) a threat warning generated by internal systems;

(b) a vulnerability announcement issued by a software or hardware provider;

(c) international warnings of cyber security threats, vulnerabilities or incidents;

(d) a system failure where the reason for the failure cannot be traced or may have been the result of a cyber security event.

(3) The Interpretation and Standard Provisions (Bailiwick of Guernsey) Law, 2016 applies to the interpretation of these Rules.

(4) A reference in these Rules to an enactment should be taken to include any amendments, re-enactments (with or without modification), extensions and applications.

**8.2 Transitional Arrangements, Citation and Commencement**

8.2.1Transitional Arrangements

(1) Firms must implement changes to their Internal Controls to ensure compliance with the Rules by 9th August 2021

8.2.2 Citation and Commencement

(1) These rules may be cited as the Guernsey Financial Services Commission Cyber Security Rules, 2021.

(2) These rules come into force on 8th February 2021.

**Materiality**

The Commission recognises the requirement for the use of judgement when considering various matters within the Rules and this guidance, specifically when considering the terms "trigger event" and "cyber security event".

For example, the Commission would expect that a Firm operating an advanced network monitoring tool would be likely to generate a significant number of threat warnings. However, it would not be expected to treat all those threat warnings as trigger events. Likewise, an internal report of a Firewall or Antimalware system blocking a virus should not automatically be considered a cyber security event.