GUERNSEY FINANCIAL SERVICES COMMISSION

CYBER SECURITY RULES, 2020

Made:

Coming into Operation:

The Guernsey Financial Services Commission ("the Commission"), in exercise of the powers conferred on it by section 16 of The Protection of Investors (Bailiwick of Guernsey) Law, 1987; sections 33A and 33B of The Banking Supervision (Bailiwick of Guernsey) Law, 1994; sections 31A and 31B of The Regulation of Fiduciaries, Administration Businesses and Company Directors, etc (Bailiwick of Guernsey) Law, 2000; sections 38A and 38B of The Insurance Business (Bailiwick of Guernsey) Law, 2002 and sections 18, 18AA and 18AB of The Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002; (collectively "the Regulatory Laws") makes the following Rules.

Contents

PART 1 – INTRODUCTION

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, 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.

PART 2 - IDENTIFY

2.1 Risk Assessment of Cyber Vulnerabilities

(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.

PART 3 – PROTECT

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 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.

PART 4 – DETECT

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.

PART 5 – RESPOND

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.

PART 6 – RECOVER

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.

PART 7 – NOTIFICATION

7.1. Notification to the Commission

(1) A licensee must notify the Commission 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.

PART 8 – 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[1] 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. Citation and commencement

(1) These rules may be cited as the Guernsey Financial Services Commission Cyber Security Rules, 2020.

(2) These rules come into force on ********.

Dated this

C.A. SCHRAUWERS
Chairman of the Guernsey Financial Services Commission
For and on behalf of the Commission

[1] Order in Council No. V of 2018, as amended.