

The Cyber Security Rules and Guidance 2021

Service area / [Corporate, Cybersecurity and Data Protection](#)

Legal jurisdictions / [Guernsey](#)

Date / [March 2021](#)

Following a two year consultation, the Cyber Security Rules, 2021 (the “Rules”) came into force in Guernsey on 5 February 2021. On 15 February 2021, the Guernsey Financial Services Commission (the “Commission”) published the consolidated Rules and guidance, The Cyber Security Rules and Guidance 2021 (the “Rules and Guidance”) under Guernsey’s regulatory laws¹ (the “Regulatory Laws”), which will ensure the Bailiwick’s regulatory regime complies with technical standards developed by international organisations.

The principle based Rules and Guidance replace the previous cyber security guidance issued by the Commission and focus on five core principles outlined in a number of international cyber security frameworks. The Rules have direct application to all licensees who are licensed under the Regulatory Laws and require licensees to “**identify, protect, detect, respond and recover**” from cyber security risks. There is also a requirement for licensees to notify the GFSC of any cyber-attacks, defined in the Rules as “*any occurrence which threatens, or has the potential to threaten, the confidentiality, integrity or availability of any IT assets or services utilised by a licensee in the course of its business*”.

Licensees have until 9 August 2021 under the transitional period in the Rules to make the necessary changes to their internal controls and procedures to identify, assess and manage cyber security risks on an ongoing basis consistent

with minimum licensing requirements. The board of directors (or equivalent) of the licensee are responsible for ensuring that the Rules are followed and all licensees must be able to provide evidence to the Commission on request that the Rules have been considered and implemented in accordance with the size, nature and complexity of the licensee’s business.

The Guidance provides boards with examples of how a firm may satisfy the requirements laid out in the Rules and may also be used by non-licensed firms such as Prescribed Businesses or Non-Regulated Financial Services Businesses. However, as above, it remains the responsibility of the board to ensure that the regulated firm complies with the Rules, even when operations are or have largely been outsourced.

Cyber security attacks have the potential to inflict significant damage on businesses and their reputations. If you need any advice or assistance in connection with the policies and procedures that are required to be put in place under the new Rules, please do not hesitate to get in touch with your usual Carey Olsen contact.

¹ The Protection of Investors (Bailiwick of Guernsey) Law, 1987 (as amended), The Banking Supervision (Bailiwick of Guernsey) Law, 1994, The Regulation of Fiduciaries, Administration Businesses and Company Directors, etc (Bailiwick of Guernsey) Law, 2000, The Insurance Business (Bailiwick of Guernsey) Law, 2002 and The Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002.

OFFSHORE LAW SPECIALISTS

BERMUDA BRITISH VIRGIN ISLANDS CAYMAN ISLANDS GUERNSEY JERSEY
CAPE TOWN HONG KONG LONDON SINGAPORE



FIND US

Carey Olsen (Guernsey) LLP
PO Box 98
Carey House
Les Banques
St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272

E guernsey@careyolsen.com



FOLLOW US

Visit our corporate team at
careyolsen.com



PLEASE NOTE

This briefing is only intended to provide a very general overview of the matters to which it relates. It is not intended as legal advice and should not be relied on as such. © Carey Olsen (Guernsey) LLP 2021. The Board should also be aware of any data protection implications arising from cyber attacks and manage them in accordance with the Data Protection (Bailiwick of Guernsey) Law, 2017. Please do not hesitate to contact your usual Carey Olsen contact in case of data protection queries.