Global Data and Cyber Handbook - Hong Kong

Security Requirements and Breach Notification

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 31 December 2024*

Yes.

appropriate technical, physical and/or organizational security controls

reasonable security controls

general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

The PDPO requires data users to take all practicable steps to ensure that any personal data held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use.

# Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 31 December 2024*

financial services requirements

providers of critical infrastructure (upon the CI Bill entering into force)

other

Under the CI Bill, CIOs are subject to a number of organizational and preventative obligations to protect the security of their CCSs, for example:

setting up a computer-system security management unit to manage the security of CCSs;

formulating and implementing a computer-system security management plan; and

conducting regular computer-system risk assessments and audits.

The precise compliance obligations applicable to a particular CIO will be set out in a Code of Practice to be issued the CI Commissioner and/or any of the Designated Authorities, as the case may be.

See also examples of sector-specific requirements below.

**Financial Institutions** - Various regulatory guidelines and circulars issued by the HKMA require institutions authorized by the HKMA such as licensed banks, restricted license banks and deposit-taking companies (collectively known as "authorized institutions" or "AIs") to comply with comprehensive technology risk management requirements, including the performance of an independent quality assurance review for major technology-related projects. See, for example, the recently released [Module TM-C-1 “Supervisory Approach on Cyber Risk Management” of the HKMA's Supervisory Policy Manual](https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20241129e2a1.pdf) and [Module TM-G-1 "General Principles for Technology Risk Management" of the HKMA's Supervisory Policy Manual](https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf). In addition, the HKMA has launched a "cybersecurity fortification initiative," which has introduced, among other things, a cyber-resilience assessment framework against which AIs are generally expected to assess their cyber resilience.

**Financial Intermediaries** - There are general requirements under the SFC [Code of Conduct and the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission](https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/management-supervision-and-internal-control-gu/management-supervision-and-internal-control-guidelines-for-persons-licensed.pdf), which include requirements such as having internal control procedures and financial and operational capabilities which can be reasonably expected to protect their operations and their clients and other licensed or registered persons from financial loss arising from theft, fraud, and other dishonest acts, professional misconduct or omissions. From time to time, the SFC also issues guidance relating to cyberattacks that may apply to specific businesses (like internet trading) or situations (like remote office arrangements) (for example, the [Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading](https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf)).

**Insurance** - The [Guideline on Cybersecurity](https://www.ia.org.hk/en/legislative_framework/files/GL20.pdf) (GL 20) issued by the Insurance Authority of Hong Kong (IA) sets out the minimum standards for cybersecurity that authorized insurers are expected to have in place to protect their business data and the personal data of their existing and potential policyholders and to ensure continuity of their business operations including a resilient cybersecurity strategy and framework tailored to mitigate relevant cyber risks that are commensurate with the nature, size and complexity of their business. Similar requirements relating to cyber security are also set out in the [Guideline on Corporate Governance](https://www.ia.org.hk/en/legislative_framework/files/GL10.pdf) (GL 10) issued by the IA as part of an effective corporate governance of authorized insurers to manage cyber security risks.

# Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

Data privacy

Securities or public company

health

financial services

# Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 31 December 2024*

No

However, the PCPD issued non-binding [Guidance on Data Breach Handling and Data Breach Notifications](https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf) in June 2023, which provides a comprehensive guide to preventing, handling and reporting data breaches.

# Controllers/Owners have to notify:

*Last updated date: 31 December 2024*

N/A

# Processors/Agents have to notify:

*Last updated date: 31 December 2024*

N/A

# Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 31 December 2024*

Yes

**Financial Institutions** - Various regulatory guidelines and circulars issued by the HKMA, Hong Kong's banking regulator, require AIs to promptly report any significant/material incidents (e.g., security breaches, data leakage, etc.) to the HKMA and/or other authorities or customers. Similar requirements apply to other HKMA-regulated entities, for example, HKMA-licensed stored value facility issuers.

**Financial Intermediaries** - Various regulatory guidelines and circulars issued by the SFC require financial intermediaries which are licensed or registered with the SFC to promptly report any significant/material incidents to the SFC and/or other authorities or customers.

**Insurance** - The IA has issued a [Guideline on Cybersecurity](https://www.ia.org.hk/en/legislative_framework/files/GL20.pdf) (GL 20), which requires that upon detection of a cybersecurity incident, an authorized insurer should report the incident with the related information to the IA as soon as practicable and in any event, no later than 72 hours from detection.

**CIOs** – Under the CI Bill, CIOs are required to report computer-system security incidents in respect of a CCS of a CI operated by the CIO to the CI Commissioner as soon as practicable and in any event within the following time limits:

If the incident has disrupted, is disrupting or is likely to disrupt the core function of the CI concerned: 12 hours after the CIO concerned becomes aware of the incident

In any other case: 48 hours after the CIO concerned becomes aware of the incident

cybersecurity authorities

financial services requirements

providers of critical infrastructure

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.