SmartSuite

Framework / Cybersecurity / Other

SFC Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading

The SFC's Guidelines for Reducing and Mitigating Hacking Risks set 20 baseline cybersecurity requirements for Hong Kong firms offering internet trading.



What it is

The Securities and Futures Commission (SFC) of Hong Kong published the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading as baseline cybersecurity requirements for firms whose clients trade over the internet. They apply to persons licensed by or registered with the SFC for Type 1, 2 or 3 regulated activity, and for Type 9 to the extent they distribute funds through internet-based trading facilities. Two-factor authentication took effect on 27 April 2018 and the other requirements on 27 July 2018.

At a glance

PUBLISHER
Securities and Futures Commission (SFC), Hong Kong

TYPE
Guidance

VERSION
Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (27 October 2017)

EFFECTIVE
April 27, 2018 (two-factor authentication); July 27, 2018 (all other requirements)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Hong Kong

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: 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

Why it matters

- **Two-factor login comes first** Requirement 1.1 calls for two-factor authentication for login to clients' internet trading accounts, using any two of what a client knows, has or is.
- **Clients are told quickly** Requirement 1.3 requires prompt notices of logins, password resets, trade executions, transfers to unregistered third-party accounts and changes to account information, sent through a channel different from the one used for login.
- **Patches have a clock** Requirement 2.4 says to implement security patches or hotfixes within one month following completion of testing.
- **The SFC tests firms against it** Its February 2025 thematic review reported unqualified two-factor authentication, delayed patching, weak encryption algorithms, excessive administrator access and missing audit trails.

How SmartSuite supports SFC Internet Trading Cybersecurity Guidelines

Authentication and Notification Controls

Record, per trading platform, the two-factor method (1.1) and the five client notification events (1.3), with an owner and test evidence.

Yearly Access Review

Run the yearly review of user access to critical systems and client databases (2.2) with reviewer sign-off and follow-up actions.

Patch Window Tracker

Log each patch or hotfix with its release, test completion and deployment dates against the one-month window in 2.4.

Backup and Contingency Evidence

Keep daily off-line backup records (2.8) and contingency exercises for DDoS and ransomware scenarios (2.9) with open actions.

Third-Party Provider Register

Track outsourced internet trading services, service-level agreements and their review dates (2.10) with the approving officer (3.1(h)).

Incident, Training and Oversight Record

Capture incident escalations (3.2), yearly training completion (3.3), self-assessments and officer approvals (3.1) in one reportable record.

Common framework mappings

EU DORA | ISO 27001:2022 | ISO 27002:2022 | ISO 27017 | ISO 27018 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SWIFT CSCF

Official resources

Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (PDF)

The SFC's full text of the 20 baseline requirements for internet trading cybersecurity.

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

SFC circular: cybersecurity review of licensed corporations (6 Feb 2025)

The SFC's circular and report on its 2023/24 thematic cybersecurity review of internet brokers.

apps.sfc.hk/edistributionWeb/api/circular/list-content/circular/intermediaries/supervision/doc?lang=EN&refNo=25EC7

SFC circular: phishing-resistant authentication and monitoring (9 Jul 2026)

The SFC's circular on phishing-resistant client login, device binding and surveillance, with the 8 July 2027 implementation date.

apps.sfc.hk/edistributionWeb/api/circular/list-content/circular/intermediaries/supervision/doc?lang=EN&refNo=26EC35

Frequently asked questions

Who must follow the SFC internet trading cybersecurity guidelines?

Persons licensed by or registered with the SFC who are engaged in internet trading for Type 1, 2 or 3 regulated activity, and Type 9 to the extent they distribute funds through internet-based trading facilities (Introduction, paragraph 3). The Guidelines do not have the force of law, but failing to follow their spirit may reflect adversely on a person's fitness and properness (paragraph 4).

How many requirements do the Guidelines contain, and how are they grouped?

There are 20 baseline requirements in three groups: protection of clients' internet trading accounts (1.1 to 1.6), infrastructure security management (2.1 to 2.10) and cybersecurity management and supervision (3.1 to 3.4). The SFC calls them minimum standards that are not exhaustive (paragraph 5).

 © 2026 SmartSuite Inc. All rights reserved.

When did the requirements take effect?

The SFC announced the Guidelines on 27 October 2017. Two-factor authentication for client login took effect on 27 April 2018, and all other requirements on 27 July 2018.

Is a one-time password still acceptable for client login?

Requirement 1.1 calls for two-factor authentication. In its 9 July 2026 circular the SFC says it does not consider an OTP phishing-resistant and expects internet brokers to adopt phishing-resistant login and device binding as soon as practicable and no later than 8 July 2027, with large internet brokers expected to move immediately.

How quickly must security patches be applied?

Requirement 2.4 says to monitor and evaluate patches and hotfixes, test them as soon as practicable and implement them within one month following completion of testing. The SFC's 2 June 2026 circular asks firms to expedite patching and to handle urgent fixes outside routine cycles.

License included / downloadable: Yes The Guidelines are published free of charge by the SFC on its website and are included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/hong-kong-sfc-cybersecurity-guidelines-for-internet-trading