

Standard of conduct expected of licensed corporations (LCs) in relation to phishing detection and prevention, end-of-life software management, remote access, Third Party Provider management and cloud security

Phishing detection and prevention

LCs should:

- (a) deploy anti-malware solutions to all servers and workstations, irrespective of the operating systems used, and update the malware signature files of these anti-malware solutions on a timely basis;
- (b) not send electronic messages (such as emails or SMS) with embedded hyperlinks that direct clients to their websites or mobile applications to undertake transactions, and not ask clients to provide via hyperlinks sensitive personal information, including login credentials and OTPs;
- (c) keep abreast of the latest cybersecurity attacks, refer to the relevant materials published by international standard setters such as National Institute of Standards and Technology¹ (NIST) and utilise local resources including CyberDefender² and InfoSec³;
- (d) provide regular cybersecurity awareness training to all staff, where phishing should be included as one of the training topics;
- (e) send clients regular cybersecurity alerts and reminders, including security reminders against phishing attacks; and
- (f) ensure their cybersecurity incident handling and reporting policies and procedures cover phishing attack scenarios that could lead to complete system shutdowns or data leakage, and specify the internal escalation and external reporting procedures.

End of life (EOL) software management

LCs should:

- (a) develop policies and procedures on IT asset management which cover, amongst other things, the identification and monitoring of the EOL or close to EOL status of the software in use, software upgrade or migration strategy and the corresponding remedial plans in managing obsolete software, where appropriate;
- (b) maintain a complete IT asset inventory list and review this list at least annually to

¹ Anti-phishing guidance from NIST: <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>

² Guidance notes from Cyberdefender: https://cyberdefender.hk/en-us/phishing_attack/

³ Knowledge centre on phishing attacks from InfoSec: <https://www.infosec.gov.hk/en/knowledge-centre/phishing>

ensure its completeness;

- (c) monitor the validity of existing software on an ongoing basis, eg, by gathering EOL relevant information from official sources of software providers⁴ in a timely manner;
- (d) maintain a complete and up-to-date EOL list for all relevant IT assets and proactively plan for replacing or upgrading software that is EOL or close to EOL, where appropriate; if LCs require additional time to address technical compatibility issue or business operational concern, and thus could not update or replace the software before it becomes EOL, the LCs should adopt the tactical measure to subscribe for extended support from software providers to ensure the availability of security patches or hotfixes; and
- (e) cease the use of EOL software on all critical system servers and databases, including internet-facing servers (eg, web servers) and trading related servers and databases. LCs should also upgrade or replace other EOL software in a timely manner (ie, those not on critical system servers and databases), unless they could properly mitigate the corresponding cybersecurity risk.

Remote access

LCs should:

- (a) develop policies and procedures on remote access management to cover, amongst other things, the requirements of remote access assignment, approval, and monitoring;
- (b) grant remote access rights on a “least privileged” and “need-to-have” basis;
- (c) remove unnecessary remote access rights in a timely manner, and ensure that LCs’ senior management, including MIC-IT, or their delegates review the list of users granted remote access, including external parties (ie, business partners and Third Party Providers) and contract staff, on a regular basis (at least annually);
- (d) implement adequate security controls over remote access to its internal network, and in particular:
 - only allow remote access via VPN or other technical solutions that provide the same security protection, such as Virtual Desktop Infrastructure;
 - implement multi-factor authentication (with at least two factors) to ensure that only authorised users can access the network or sensitive data repositories; ensure that passwords, if used as one of the authentication factors, are subject to the same password policies as stipulated in the Cybersecurity Guidelines; and

⁴ For example, <https://access.redhat.com/support/policy/updates/errata> for Linux-related resources and <https://learn.microsoft.com/en-us/lifecycle/overview/product-end-of-support-overview> for Microsoft Windows related resources as reference.

- implement session timeout control requirements.

When granting remote access to Third Party Providers, LCs should:

- (a) not grant them permanent access rights; and
- (b) log and monitor Third Party Providers' remote connection to LCs' internal networks and the activities undertaken.

LCs should comply with the expected standards on remote access set out in the "Report on Operational Resilience and Remote Working Arrangements"⁵.

Third Party Provider management

LCs should:

- (a) develop policies and procedures on Third Party Provider management, including Third Party Provider due diligence, selection and approval, contract management, performance monitoring, risk management (including cybersecurity risk management), compliance with regulatory requirements, dispute resolution, termination and exit strategy, and record keeping;
- (b) maintain a complete list of Third Party Providers, including the name, contact details and description of services provided, to facilitate ongoing Third Party Provider management and monitoring;
- (c) conduct proper due diligence on Third Party Providers prior to appointment, and in particular, assess the adequacy of the cybersecurity measures implemented by the Third Party Providers;
- (d) enter into a formal service-level agreement (SLA) with Third Party Providers which specifies the terms of service and the responsibilities of the providers, particularly:
 - the cybersecurity measures to be implemented by the providers; and
 - the reporting procedures for cybersecurity incidents;
- (e) regularly review and where appropriate revise the SLA to reflect any changes to the outsourcing arrangements or regulatory developments;
- (f) monitor the performance of the Third Party Providers on a regular basis to identify any non-compliance with the SLA or unsatisfactory performance in a timely manner;
- (g) set the security control configurations and parameters utilised in the systems supplied by Third Party Providers in compliance with the relevant requirements,

⁵ https://www.sfc.hk/-/media/EN/files/COM/Reports-and-surveys/Report_Operational-resilience-and-remote-working-arrangements_Oct-2021_EN.pdf

including the Cybersecurity Requirements; and

- (h) incorporate into their business contingency plans the unavailability of services provided by the Third Party Providers and related cybersecurity scenarios and corresponding contingency strategies. Where possible, they should conduct regular drills and recovery tests together with these providers.

Cloud security

LCs should:

- (a) develop policies and procedures on cloud security management which include access credential management, secured cloud infrastructure, data encryption, security logging and monitoring, backup, compliance controls, regular audits and incident response and reporting;
- (b) conduct proper due diligence on the third-party cloud service providers, particularly the security controls implemented by these providers;
- (c) implement a secure network infrastructure⁶ and properly segregate the network segment or security group hosting critical systems and data from other network segments or security groups that are subject to higher hacking risk exposure⁷;
- (d) implement adequate controls to guard against unauthorised access and usage of the root account of the cloud platform⁸; and put in place sufficient controls, such as two-factor authentication and IP whitelisting, to prevent unauthorised access and usage of this account;
- (e) properly secure and manage the cloud access credentials, which include application programming interface (API) keys and access tokens, for interacting with internet trading systems and data and grant the access rights assigned to these credentials on a “need-to-have” and “least privilege” basis. LCs should also apply this expected standard to data access and communication between application systems on different clouds (eg, between trading system and settlement system);
- (f) change API keys regularly, and avoid using permanent keys;
- (g) back up business records, client and transaction databases, servers and supporting documentation in an offline medium at least on a daily basis; also ensure that the backup is “immutable”, ie, Write-Once-Read-Many (WORM) and

⁶ The design and implementation of network infrastructure to host systems and data in the cloud environment would be different from the network infrastructure set up in the “non-cloud” environment, eg, on-premises data centre. Hence, LCs may not necessarily deploy the network segmentation through a typical demilitarised zone with multi-tiered firewalls. They should use cloud-native segmentation controls and adopt micro-segmentation approach to deploy the network segmentation in a granular manner, ie, access restriction between segregated network clusters, security groups and even individual system service and component.

⁷ For example, web servers or internet-exposed services.

⁸ Root account of cloud computing platform is the highest privileged account with full access to all system services and resources in the cloud environment.

“air-gapped”, ie, the backup medium should be disconnected from the cloud environment after each backup process; and

- (h) collaborate with third-party cloud service providers to formulate the cloud-related cybersecurity and unavailability scenarios in their business contingency plans, and where possible, coordinate with the third-party cloud service providers when performing drills and recovery tests.