NSDL
Technology, Trust & Reach

Participant Services
Circular

Circular No.: NSDL/POLICY/2023/0139 October 04, 2023

Subject: Advisory for SEBI Regulated Entities (REs) regarding Cyber Security best practices.

Attention of Participants is invited to SEBI circular No.: SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023 read with NSDL Circular No.: NSDL/POLICY/2023/0027 dated February 23, 2023 regarding **"Advisory for SEBI Regulated Entities (REs) regarding Cyber Security best practices".**

In this regard**,** Participants are hereby informed that the format has been prescribed to submit compliance status of Cyber Security best practices advisory issued through above mentioned circular and same is enclosed as **Annexure – A.**

Participants are advised to submit the compliance report to NSDL at dpaudit@nsdl.com **on or before October 31, 2023** for the FY 2023-2024.

Participants are requested to take note of the above and ensure compliance.

For and on behalf of
National Securities Depository Limited

Digitally signed by AROCKIARAJ
Date: 2023.10.04 17:39:38 +05'30'

Arockiaraj
Manager

Enclosed: One

FORTHCOMING COMPLIANCE			
Particulars	**Deadline**	**Manner of sending**	**Reference**
Investor Grievance Report (Monthly)	By 10th of the following month	Through e-PASS	Para 20 of NSDL Master Circular for Participants on 'Grievance Redressal' chapter
Networth Certificate and Audited Financial Statements (yearly)	October 31st	Through e-PASS	Para 27 of NSDL Master Circular for Participants on Internal Controls/Reporting to NSDL / SEBI chapter and Circular Nos. 1.NSDL/POLICY/2023/0069 dated June 16, 2023, 2.NSDL/POLICY/2023/0122 dated September 11, 2023 3.NSDL/POLICY/2023/0131 dated September 25, 2023.
Artificial Intelligence /Machine Learning Reporting Form (if offering or using such technologies as defined) (Quarterly)	By 15th of the following month.	Through e-PASS	Para 10 of NSDL Master Circular for Participants on 'Internal Controls/Reporting to NSDL/SEBI' chapter
Cyber Security & Cyber Resilience framework of Depository Participants (-Quarterly)	By 15th of the following month	Through e-PASS	Para 2.59 of NSDL Master Circular for Participants on 'Internal Controls/Reporting to NSDL/SEBI' chapter

Internal/ Concurrent Audit Report (April - September)	November 15th every year	Through e-PASS	Para 20.4 of NSDL Master Circular for Participants on 'Internal Controls/Reporting to NSDL/SEBI' chapter
Risk Assessment Template (April - September)	October30th every year.	Through e-PASS	Para 7 of NSDL Master Circular for Participants on 'Internal Controls/Reporting to NSDL/SEBI' chapter
Reporting of status of the surveillance alerts generated by Participants- (Quarterly)	Within 15 days from end of the quarter	Through e-PASS	Para 11.7 of NSDL Master Circular for Participants on 'Internal Controls/Reporting to NSDL/SEBI' chapter

ANNEXURE - A

In view of the increasing cybersecurity threat to the securities market, SEBI Regulated Entities (REs) are advised to implement the following practices as recommended by CSIRT- Fin.

Sr. No.	Requirement	Compliant/Non-Compliant/Not Applicable	Remark (To justify why points are Not Applicable)
1.	**Roles and Responsibilities of Chief Information Security Officer (CISO)/ Designated Officer:** REs/Member are advised to define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.		
2.	**Measures against Phishing attacks/ websites:** i. The REs/Member need to proactively monitor the cyberspace to identify phishing websites w.r.t. to REs/Member domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.		
	ii. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.		

3.	**Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):** i. All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.		
	ii. Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time. The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.		
4.	**Measures for Data Protection and Data breach:** i. REs/Member are advised to prepare detailed incident response plan.		
	ii. Enforce effective data protection, backup, and recovery measures.		
	iii. Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.		
	iv. Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.		
	v. Deploy data leakage prevention (DLP) solutions / processes.		

5.	**Log retention:** Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. REs/Member are advised to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done. Refer SEBI circular CIR/MIRSD/24/2011 dated December 15, 2011.		
6.	**Password Policy/Authentication Mechanisms:** i. Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex- employees Passwords should not be reused across multiple accounts or list of passwords should not be stored on the system.		
	ii.Enable multi factor authentication (MFA) for all users that connect using online / internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.		
	iii. Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.		
7.	**Privilege Management:** i Maker-Checker framework should be implemented for modifying the user's right in internal applications. ii. For mitigating the insider threat problem, 'least privilege' approach to provide security for both on- and off-premises resources (i.e., zero-trust models) should be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or		

	outside of a network perimeter.		
8.	**Cybersecurity Controls:** i. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.		
	ii. Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.		
	iii. Restrict execution of “powershell” and “wscript” in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.		
	iv. Utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.		
	v. Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.		
9.	**Security of Cloud Services:** i. Check public accessibility of all cloud instances in use. Make sure that no server/bucket is		

	inadvertently leaking data due to inappropriate configurations.		
	Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.		
	ii. Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.		
	iii. Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.		
10.	**Implementation of CERT-In/ CSIRT-Fin Advisories:** The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.		
11.	**Concentration Risk on Outsourced Agencies:** i. It has been observed that single third party vendors are providing services to multiple Res/Members, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyberattack, happens at such organizations, the same could have systemic implication due to high concentration risk.		
	ii. Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate		

	such concentration risk. Further, REs/Member also need to take into account this concentration risk while outsourcing multiple critical services to the same vendor.		
12.	**Audit and ISO Certification:** i. SEBI's instructions on external audit of REs/Member by independent auditors empanelled by CERT-In should be complied with in letter and spirit.		
	ii. The REs/Member are also advised to go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE/Member with respect to cybersecurity.		
	iii. Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits		

I/We hereby confirm on compliance to the Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices recommended by CSIRT-Fin through SEBI Circular No: SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032, Dated February 22, 2023.

I/We certify that all the statements are true and correct to the best of our knowledge.

***