METROPOLITAN STOCK EXCHANGE

Department: Technology	**Segment: All Segments**
Circular No: MSE/IT/17145/2025	**Date: May 08, 2025**

Subject: Cyber Safety Measures

Advisory - This data is to be considered as TLP: AMBER

To All Members,

On the backdrop of recent developments impacting national security, Metropolitan Stock Exchange of India (MSEIL) recommends Members to have sharp focus on cyber security, following are the measures below but not limited to:

1. **Action on Alerts & Advisories**: Promptly act on alerts and advisories issued by the Government, CERT-In, NCIIPC, SEBI, Exchanges, etc.

2. **24*7 Monitoring**: Switch to heightened alert mode with 24*7 Security Operations Center (SOC) and Network Operations Center (NOC) monitoring. Ensure near 100% manpower availability and a high state of readiness for proactive threat detection and mitigation. Regularly examine logs of web servers and perimeter devices (e.g., WAF, firewall, DNS) to detect malicious requests or traffic.

3. **Monitor Privileged Accounts**: Closely monitor all privileged accounts for unauthorized access. Enforce a least privilege policy for these accounts.

4. **Backup Critical Data**: Maintain offline, encrypted backups of all critical information infrastructure and business-critical assets. Store copies of Backup at different locations.

5. **Activation of Incident Response/Cyber Crisis Management Plan**: Ensure Incident Response (IR) teams are ready to respond to any cyber incident.

6. **Patch Management**: Keep all applications, operating systems, and hardware updated with latest patches. Regularly prioritize and manage patches for vulnerabilities that could be exploited.

7. **Threat Hunting**: Conduct proactive threat hunting to identify and eliminate any compromise or persistence of threat actors in your systems.

8. **MSPs/Vendors on High Alert**: Sensitize Managed Service Providers (MSPs) and vendors to adhere to cyber security practices and deploy high-quality manpower and standby teams for response.

9. **Access Controls**: Enforce Multi-Factor Authentication (MFA) across all accounts where feasible. Disable non-essential user access and third-party integrations.

10. **DDoS Mitigation**: Protect web-facing information infrastructure, including web portals and websites, against DDoS attacks by implementing proper mitigation tools and considering clean pipe solutions from ISPs. Implement geo-fencing based on business requirements.

11. **Special Watch on Phishing**: Monitor emails for phishing attacks. Report all phishing emails and ensure vigilance/reporting of phishing websites.

12. **Employee Sensitization**: Educate employees to be alert and report any phishing attempts, credential theft, or suspicious activities on organizational systems.

13. **Cyber Drills**: Test the effectiveness of the Incident Response Plan (IRP) and Cyber Crisis Management Plan (CCMP) by conducting cyber drills, especially against ransomware and DDoS attacks. Use identified gaps to update the CCMP.

14. **Attack Surface Management and VA**: Regularly conduct Vulnerability Assessments (VA) to identify security gaps. Perform continuous red teaming to find and fix vulnerabilities before they can be exploited by threat actors.

15. **Redundancy Activation**: Ensure high availability of critical assets and services to maintain business continuity in case of any contingency.

Specific Security Action Points to consider but not limited to:

Web Server & Infrastructure Hardening	**Monitoring & Alerts**
• Block all unused ports (e.g. 23, 445, 3389) on servers, firewalls, and cloud instances. • Disable RDP/SSH from the internet — only allow access via VPN or internal IPs. • Scan all web servers and infrastructure for open ports and known vulnerabilities (use tools like Nmap, OpenVAS).	• Enable login attempt alerts on sensitive systems (e.g., VPN, admin panels). • Monitor logs for failed login attempts, config changes, and new device connections. • Block IPs showing brute-force activity using firewall or endpoint rules. • Watch for abnormal traffic spikes from foreign or domestic IPs — investigate and isolate if needed.

• If a patch is not possible, protect exposed systems using custom WAF or firewall rules. • Remove or isolate unmaintained, old, or unused web applications and systems. • Apply the latest OS, software, and firmware updates across all systems.	
Access Control, Network & System Protection • Enforce strong passwords (minimum 12 characters; no reuse). • Enable Multi-Factor Authentication (MFA) on email, VPN, admin panels, and cloud platforms. • Remove ex-employee access and disable all unused accounts. • Restrict admin privileges to essential personnel only. • Use VPNs or any other secure access methods for all remote access.	**Geo & Threat-Based IP Blocking** • If not critical to business, block incoming traffic from high-risk countries using firewall or CDN geo-filters.

This document is distributed as TLP: *AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.*

Disclaimer:

The information provided by Metropolitan Stock Exchange of India Limited above is on "need to know" basis only. System Administrators are advised to independently evaluate the contents for its applicability in their specific environment and take appropriate action as per their own assessment of the implications of the alert/ advisory on their information technology eco system. Metropolitan Stock Exchange of India Limited will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System Administrators are wholly responsible for cyber security updates to their information technology eco system.