# Central Depository Services (India) Limited

**Convenient ⌖ Dependable ⌖ Secure**

**COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS**

**CDSL/OPS/DP/POLCY/2025/297** **May 06, 2025**


## ADVISORY FOR CYBER SECURITY PREPAREDNESS

In light of the ongoing current geopolitical situation**,** we urge all Depository Participants to remain **extra vigilant** against potential cyber threats. During such period, threat actors often exploit uncertainty to launch **phishing attacks**, spread **misinformation**, and attempt to **compromise systems and data**.

To safeguard your organization and your personal digital security, you are advised to follow the cybersecurity guidelines mentioned below:

**1. Issue a Security Alert to All Staff**

- Inform employees of the increased risk of phishing, social engineering, or malware.
- Remind them not to trust and report system anomalies, unusual links, or requests for sensitive information.

**2. Patch Critical Vulnerabilities**

- Apply all relevant security patches and firmware updates promptly.
- Prioritize fixes for internet-facing and critical systems (VPNs, firewalls, email servers, etc).

**3. Enhance Threat Monitoring**

- Act swiftly on alerts from brand monitoring tools. These alerts may indicate phishing campaigns or impersonation attempts targeting the organization or high-profile personnel.
- Activate 24/7 security operations centre (SOC) or assign an on-call response team.
- Increase real-time monitoring using SIEM tools for unusual login attempts, data exfiltration, or system changes.
- Exercise caution with macro-enabled Excel files, particularly those with the .XLAM extension. These are Excel add-ins that load automatically and may contain embedded malicious code. Attackers often use them as a stealthy delivery mechanism for malware.
- Restrict powershell usage within the organisation.
- Closely monitor your systems for DDoS alerts. Reduce exposure of your applications on the Internet.
- Report any anomalies immediately, including unusual system behaviour, unauthorized login attempts, or suspicious user activity. Prompt notification to the Security Operations Centre (SOC) is critical for early detection and response.

**4. Tighten Access Controls**

- Enforce least privilege access—only essential personnel should access critical systems.
- Temporarily restrict admin-level access unless absolutely required.

**5. Secure Backup Systems**

- Ensure offline, immutable, or cloud-based backups are in place and tested.

**6. Strengthen Endpoint Security**

- Ensure all endpoints (laptops, desktops, servers,) have updated antivirus, EDR, and firewall rules.
- Block unauthorized USB devices or removable media.

**7. Cyber Incident Response Plan**

- Review your team's response time, communication flow, recovery actions, corrective and preventive measures.

**8. Coordinate with External Agencies**

- Report incidents to CERT-In, SEBI and relevant authorities.
- Report real-time incidents or suspicious activity as per applicable guidelines.

Avoid forwarding unverified news or messages on social media or messing platform. Your **alertness and compliance** with these practices are essential in helping us to protect against cyber threats during these sensitive times.

For **any suspicious cyber alerts & incidents,** kindly report to the **CDSL IT Security Team** on dpincident@cdslindia.com and connect through our IVR Number 022-62343333.

**For and on behalf of**
**Central Depository Services (India) Limited**

**sd/-**

**Akhil Wadhavkar**
**Chief Information Security Officer**