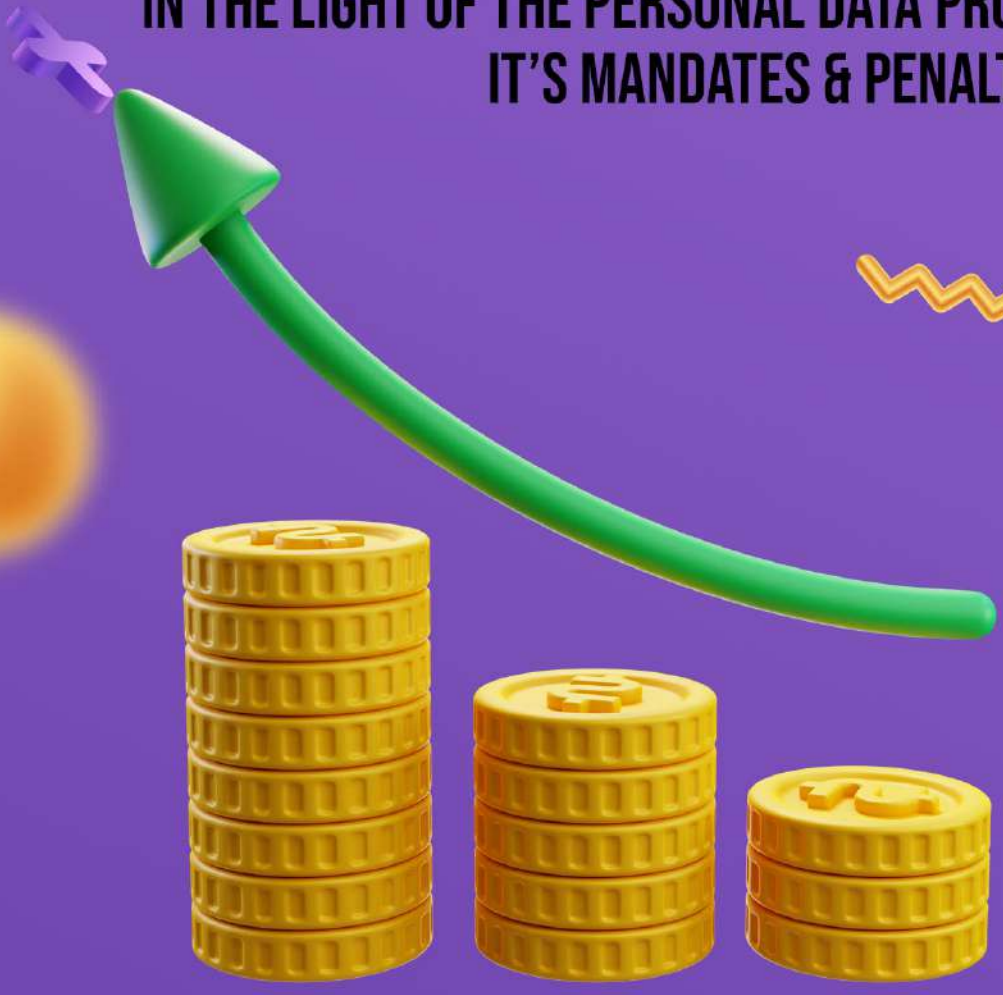
Cyberjure Legal Consulting
Simplifying Cyber Law

Enabling & Guiding you to be Cyber & Data Law Compliant

SEBI ISSUES CIRCULAR ON MANDATORY DATA & CYBER SECURITY & DARK WEB MONITORING

CIRCULAR DATED 29.08.2023

IN THE LIGHT OF THE PERSONAL DATA PROTECTION ACT,2023- IT'S MANDATES & PENALTIES



Advocate Puneet Bhasin
Cyber Law & Data Protection Expert

CONTACT US
Cyberjure Legal Consulting
www.cyberjure.com | www.puneetbhasin.in contact@cyberjure.com +91 7668528027

I. APPLICABILITY OF CIRCULAR

(i) **Stock Exchanges**
(ii) **Clearing Corporations**
(iii) **Depositories: National Securities Depositories Limited (NSDL), Central Depositories Services Limited (CDSL), Market Infrastructure Institutions.**

II. INTRODUCTION

Market Infrastructure Institutions (MIIs) such as Stock Exchanges, Clearing Corporations, and Depositories play a crucial role in ensuring the smooth operation of the securities market. Their significance lies in providing essential infrastructure for trading, clearing, and settlement. Due to their systemic importance, MIIs must prioritize robust cyber security frameworks to support their vital functions and mitigate operational risks. This includes establishing and enhancing Information Technology (IT) processes and controls to safeguard data confidentiality, integrity, and system availability. In the context of the evolving dynamics of the Indian Securities markets, the interdependence among MIIs has grown significantly. This interconnectedness highlights that the cyber risk faced by any MII extends beyond its own systems and assets. As a result, MIIs are now required to take proactive measures to implement necessary systems, even making amendments to relevant bye-laws, rules, and regulations within 120 days from the issuance of the circular. This emphasis on addressing cyber risks underscores the critical need for MIIs to collaborate and ensure the resilience of the overall market infrastructure.

III. MANDATED PRACTICES

(i) **Safeguarding Data Integrity and Availability:** MIIs must uphold offline, encrypted data backups and conduct regular tests, at least quarterly, to ensure data confidentiality, integrity, and availability.

(ii) **Gold Images:** MIIs must keep up-to-date "gold images" of vital systems for potential reconstruction. This involves having preconfigured templates with the operating system and software, facilitating swift deployment for system rebuilding, like virtual machines or servers.

(iii) **Enhancing System Reliability:** MIIs are advised to consider having extra hardware in a separate setting for system rebuilding if starting operations from both Primary Data Centre (PDC) and Disaster Recovery Sites (DRS) isn't possible. They should also maintain spare hardware ready for critical services, keeping it updated with new changes like OS and security patches from primary systems. Regular

testing in accordance with MIIs' response and recovery plan is essential for this spare hardware.

(iv) **Routine Drills and Vulnerability test:** MIIs need to conduct routine business continuity drills to assess organizational readiness and security control effectiveness against ransomware attacks. Additionally, they should regularly conduct vulnerability scanning to detect and mitigate vulnerabilities, particularly on devices accessible via the internet, in order to reduce the potential for attacks.

(v) **Continuous Software and OS Updates:** MIIs must ensure software and OSs are consistently updated to the latest versions, with a quarterly review to verify compliance.

(vi) **Training Programs:** MIIs must establish a cybersecurity training program to educate users about recognizing and reporting suspicious activities like phishing. Additionally, they should deploy email gateway filters to block emails with malicious indicators and prevent access to suspicious IP addresses, domains, and URLs through the firewall.

(vii) **Robust Endpoint Security Measures:** MIIs need to maintain updated Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP), antivirus, and anti-malware software across all IT systems. Moreover, they should implement application directory whitelisting on all assets to allow only authorized software and prevent unauthorized installations or executions.

(viii) **Enhancing Access Security:** MIIs must utilize Multi-Factor Authentication (MFA) for all services. Additionally, they should adhere to the principle of least privilege across systems and services, ensuring users have access only to necessary tasks, consider implementing Privileged Identity Management (PIM)/Privileged Access Management (PAM) solutions.

(ix) **Elevating Efficiency and Security:** Market Infrastructure Institutions (MIIs) can enhance operational efficiency and security by adopting a configuration management database approach. This involves cataloging IT assets—both intangible (data, software) and tangible (hardware)—enabling better resource management. Moreover, the approach aids in identifying crucial data/systems for critical services and understanding interconnections among them, leading to the creation of a comprehensive "critical asset/system list." These measures empower MIIs to ensure seamless operations and stronger security

(x) **Strengthening Active Directory Security:** MIIs need to consistently audit the Active Directory (AD) to identify and address existing vulnerabilities like compromised service accounts, which could be exploited by attackers due to their administrative privileges.

(xi) **Securing domain controllers (DCs)**: Securing domain controllers (DCs) is of paramount importance as threat actors frequently target these as a launching pad for

spreading ransomware throughout the network. MIIs must implement a multi-faceted strategy to bolster DC security:

a) Regular patching of DCs is crucial, and the adherence to patch releases should be verified quarterly.
b) Avoid installing unnecessary software on DCs to minimize the risk of unauthorized code execution.
c) Restrict access to DCs solely to the Administrators group. Within this group, users should have limited access, utilizing separate accounts with non-administrative privileges for day-to-day activities.
d) Configure DC host firewalls to prevent direct internet access, fortifying their defense against external threats.
e) MIIs should proactively undertake penetration testing, both internally and externally, to detect and address vulnerabilities related to known Active Directory Domain Controller abuse attacks. Swift action should be taken to rectify identified weaknesses.

(xii) **Ensuring Access Accountability and Log Security:** Delegated access and unused tokens need quarterly review and cleansing. MIIs must retain and secure logs for various systems and devices, maintaining full verbosity.

(xiii) **Fortifying Network Security:** Network devices within MIIs should adhere to a whitelist configuration for communication, specifying IPs, ports, and services, enforced through Access Control Lists (ACLs). MIIs must establish effective network segregation to limit the impact of cyber incidents and reduce disruptions to operations. For secure usage, MIIs should implement Remote Desktop Protocol (RDP) on a need-only basis, employing Multi-Factor Authentication (MFA). If required, authorized personnel can access from whitelisted IPs for a predefined time, with activity logging in place.

(xiv) **Enhancing API and DNS Security:** Accessing MIIs through Application Programming Interface (API) should follow a whitelist approach. MIIs must employ an API security solution to safeguard services and data exchanged through APIs. MIIs need to enforce Domain Name System (DNS) filtering services to allow clean DNS traffic in their environment. Utilizing Domain Name System Security Extensions (DNSSEC) is crucial for secure communication.

(xv) **Restricted Access Paradigm**: Access to critical servers, applications, services, and network elements should be limited exclusively to enterprise-recognized intranet systems.

(xvi) **Streamlining Threat Intelligence Integration:** MIIs must establish mechanisms to integrate and manage IOCs/malware alerts/vulnerability alerts received from CERT-in, NCIIPC, linked MIIs, or government agencies. MIIs are required to formulate standard operating procedures (SoP) for promptly

implementing advisories from CERT-In, NCIIPC, or government agencies within a set timeframe. These procedures should be shared with SEBI.

(xvii) **Enhancing Resilience through Rigorous Testing:** MII's response and recovery plan needs regular review and testing, encompassing a range of scenarios including extreme yet feasible cyber-attacks. These tests must challenge assumptions about response, resumption, and recovery processes, involving governance and communication plans. They should involve critical service providers, vendors, and linked MIIs. MIIs should consider operating systems on diverse application architectures to ensure high availability during disasters.

IV. DARK WEB MONITORING

Market Infrastructure Institutions (MIIs) are advised to consider employing Dark Web monitoring services as a part of their cybersecurity strategy. These monitoring services play a crucial role in identifying potential threats that might emerge from the dark corners of the internet. The dark web, often hidden from traditional search engines, serves as a breeding ground for cybercriminal activities, including brand abuse, data leaks, and credential exposures. By engaging Dark Web monitoring services, MIIs can proactively stay vigilant against any instances of brand abuse, wherein threat actors might attempt to exploit the institution's name or image for malicious purposes. Furthermore, these services help in detecting instances where sensitive data or credentials belonging to the institution might have been compromised and are being traded or sold on illicit platforms. Such data leaks and credential exposures can have severe consequences for an institution's reputation and security posture.

V. CONCLUSION

In response to the escalating interdependency within the market, these guidelines have been introduced as a necessary measure to fortify the security posture of Market Infrastructure Institutions (MIIs). The evolving landscape of the Indian Securities markets has witnessed a substantial surge in the interconnectedness and reliance among MIIs. This shift highlights that the vulnerability of any MII to cyber risks extends beyond its own systems and assets, rendering a holistic approach to security imperative.

Among the comprehensive set of 28 guidelines, several key directives are outlined. One of the focal points is the establishment of offline, encrypted data backups that are subjected to regular testing on a quarterly basis. This practice ensures the confidentiality, integrity, and availability of critical data in the event of a security breach or data loss. Additionally, the guidelines underscore the importance of considering spare hardware for system rebuilding, particularly when primary operations from designated centers might be unfeasible.

The significance of business continuity is also underscored, with MIIs urged to undertake regular drills to assess organizational readiness and the effectiveness of security controls, particularly in light of the rising threat of ransomware attacks. Furthermore, the guidelines delve into the pivotal role that domain controllers (DCs) play in cybersecurity, detailing measures to secure these systems. This includes timely patching, avoiding unnecessary software installations, restricting access, configuring firewalls, and conducting comprehensive penetration testing.

The overarching theme of these guidelines is to mitigate the risks associated with the evolving cybersecurity landscape. By implementing these directives, MIIs can enhance their resilience against cyber threats and ensure the uninterrupted functioning of critical operations. As technology and threat vectors continue to evolve, these guidelines serve as a comprehensive roadmap for MIIs to navigate the intricate realm of cybersecurity with a proactive and robust approach.

VI. DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 emerges as a historic milestone in the realm of digital rights after it was passed by the Lower House of Parliament (the Lok Sabha) and the Upper House of Parliament (the Rajya Sabha) followed by Presidential assent making it a law of the land. With privacy at its core, this landmark legislation would empower individuals, redefine business practices, and usher in a new era of responsible data handling.

The Act regulates the governance of personal data collected by organisations, and aims at protecting the individual’s privacy by empowering them with rights over the manner in which their data is processed.

We are pleased to present the overview of the Act and would be pleased to assist you in formulating your strategies and thoughts in your organisation's Personal Data Protection journey.

Key highlights:

- Lawful basis of processing consolidated to consent and certain legitimate uses
- Data localisation rules relaxed allowing transfers across jurisdictions unless specifically notified
- Data processing agreements mandatory before outsourcing activities to third parties
- Financial penalties up to Rs. 250 crore per instance of non-compliance with the law

- Periodic Data Protection Impact Assessments made mandatory for Significant Data Fiduciary
- Personal data in public domain excluded from scope.

VII. PENALTIES UNDER DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Data Protection Bill contains severe financial penalties for those that do not comply with it. Specifies penalties for various offences such as up to: (i) Rs. 200 crores for non-fulfilment of obligations for children, (ii) Rs. 250 crores for failure to take security measures to prevent data breaches, and same penalty in breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach (iii) Rs. 10,000 if a data principal fails to perform their duties as specified therein