ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

POLICY ON DATA BREACH/LEAKS

Version	**2024/01.02**
Review Date	**05/04/2024**
Review & Approved by	**Reviewed by Technology Committee & Approved by Board of Directors**

Policy Statement:

The organization registered as a Stock Broker and Depository Participant recognizes the importance of protecting client information and is committed to maintaining the confidentiality, integrity, and availability of sensitive data.
This policy establishes guidelines and procedures to prevent, detect, and respond to data breaches or leaks, ensuring compliance with regulatory requirements and minimizing the impact on clients and the organization.

1. **Data Classification:**

   a. Classify data based on sensitivity and regulatory requirements, such as personal information, financial data, and trade records.
   b. Implement appropriate security controls and access restrictions based on data classification.

2. **Security Measures:**

   a. Maintain robust cybersecurity measures, including firewalls, intrusion detection/prevention systems, encryption, and access controls, to protect against unauthorized access or data breaches.
   b. Regularly update and patch software systems to address vulnerabilities.
   c. Conduct periodic security assessments and audits to identify and mitigate risks.

3. **Data Breach/leak**

Attackers are using a variety of techniques to overcome the security systems of their targeted businesses in order to steal private data.

They try to target public-facing/external systems of businesses to ultimately gain access to the internal networks, servers and databases. Another trend which has been observed is that attackers are exfiltration data and then deploying ransomware to encrypt the data they have stolen. In such incidents, attackers also threaten to release the stolen data in public domain, if the ransom is not paid.

I. Common causes of Data breach / Data leak

The common causes of such incidents are as follows:

Misconfiguration:
Poorly configured network devices can inadvertently allow traffic that would otherwise have been blocked, while incorrect file permissions on a server could expose vital data to risk. It is also possible to send data accidentally to any wrong person, misconfigured servers and careless uploads to public folders, directory listing can also lead to data breach or leakage.
Application Vulnerabilities:
Application vulnerabilities are system flaws or weaknesses in applications that could be exploited by threat actors to compromise the security and integrity of the application.
Insider Threat:
Most insider misuse happens through misinformed / uninformed staff and disgruntled /compromised users. Although most data breaches are facilitated by external malicious actors, it is still the case that insiders with or without privileged access are playing a key role in data breaches. People make mistakes and their minor mistakes could lead to a big loss to the business. Confidential information may get distributed without using any data prevention techniques. Weak/ Default/ Stolen Credentials Stolen or default credentials are one of the easiest ways attackers get access to systems, enabling them to gain access to sensitive content and resources. Also poorly configured VPN and Work from Home methods result in compromise of legitimate accounts and further misuse.

II. Best practices to prevent data breaches:

i. Organisations are advised to prepare detailed incident response plan and 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. In addition, share the details of CISO with CERT-In through Email (info AT cert-in.org.in)

ii. Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.

iii. People have always been the weakest link in the cybersecurity chain. Provide training to employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone they shouldn't to use their corporate device-especially in Work from Home environments.

iv. Establish and maintain an incident response team and evaluate incident response plans frequently.

v. Identify and classify sensitive/personal data and apply measures for encrypting such data in transit and at rest. Deploy data loss prevention (DLP) solutions / processes.

vi. Deploy detection and alerting tools and create process to prevent, contain and respond to a data breach/ data leak.

vii. Develop and maintain strong policies enforcing strong passwords (password management) and the use of multi-factor authentication (MFA). MFA adds additional layer of security and reduces the risk of perpetrator using stolen credentials to move an attack further.

viii. Always keep up-to-date operating systems and other application software because attackers identify the bugs in old versions and use them to attack. ix. Consider using models that take the `least privilege' approach to provide security for both on-and off-premises resources (i.e. zero-trust models). 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.

ix. Micro-segmentation helps contain the movement by giving organizations increased control over lateral communication that occurs between resources. Furthermore, in the event of a breach, micro-segmentation serves to limit the possible lateral exploration of networks by bad actors.

x. Enforce BYOD security policies, like requiring all devices to use a business-grade VPN service and antivirus protection.

xi. Create policies and plans for engaging with governance, risk management and compliance teams. xiii. Evolve and implement a Data Backup policy. All the business critical data should be backed up regularly to prevent data loss and to ensure faster recovery from data breach.

Refer Cert-in Advisory for following

1. Best Practices while using Amazon's AWS S3 and EC2 services
2. Best practices while using MongoDB and Elasticsearch servers
3. Best practices for securing ELK stack instance
4. Best practices for individual users to safeguard against data breaches

III Steps to be taken when organisation/entity is affected by a data breach/data leak:

i. Disconnect the compromised system from the internet, but don't turn it off. Turning of the system could result in loss of crucial evidences which would be needed for the analysis and investigation of the incident.

ii. Ensure all credentials in an organization, including service accounts, are reset and that default passwords or those similar to previous passwords are not used.

iii. Report the data breach/ data leak to CERT-In Incident Response Help Desk immediately. (email: incident AT cert-in.org.in , see Contact us page for details)

iv. Notify users/customers who could be affected immediately with details of information breached; actions being undertaken to address the problem and how they can reach back for any queries.

4. **Incident Response Team:**

   a. Designate a cross-functional incident response team responsible for managing data breach incidents.
   b. The team should include representatives from IT, legal, compliance, operations, and management.

5. **Incident Reporting:**

   a. Establish a clear process for reporting suspected or confirmed data breaches or leaks promptly.
   b. Identify designated individuals and contact information for reporting incidents, both internally and externally.

6. **Incident Assessment and Investigation:**

   a. Conduct a prompt assessment to determine the nature, scope, and potential impact of the data breach or leak.
   b. Engage internal or external experts to conduct forensic investigations, if necessary, to identify the cause and extent of the incident.

7. **Notification and Communication:**

   a. Comply with applicable regulatory requirements regarding the notification of data breaches or leaks to affected individuals, regulatory authorities (such as SEBI), and other stakeholders.
   b. Establish procedures for notifying affected clients, including the content and timing of notifications.
   c. Communicate with clients, regulators, and other stakeholders in a transparent and timely manner, providing accurate information about the incident and the steps being taken to address it.

8. **Remediation and Recovery:**

   a. Take immediate action to contain and mitigate the breach or leak, including isolating affected systems, disabling compromised accounts, and blocking unauthorized access.
   b. Implement remedial measures to prevent similar incidents in the future, such as system upgrades, security enhancements, and staff training. c. Restore affected systems and data to a secure state.

9. **Documentation and Reporting:**

   a. Document all actions taken during the incident response process, including timelines, decisions, and communications.
   b. Prepare comprehensive incident reports that detail the cause, impact, and remediation of the data breach or leak.
   c. Provide reports to senior management, compliance officers, regulatory authorities, and clients as required.

10. **Employee Training and Awareness:**

    a. Conduct regular training programs to educate employees about data protection, security best practices, and their responsibilities in preventing data breaches or leaks.
    b. Raise awareness about the potential risks, common attack vectors, and the importance of reporting incidents promptly.

11. **Policy Review and Updates:**

    a. Periodically review and update the Data Breach/Leak Policy to incorporate changes in regulatory requirements, technology advancements, and emerging threats.
    b. Ensure ongoing compliance with SEBI regulations, other applicable data protection laws, and industry best practices.