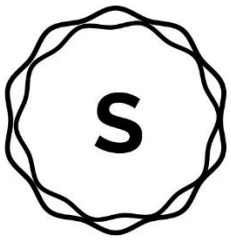

SHANNON

SHANNON ADVISORS PRIVATE LIMITED

Data Backup, Storage, and Security Policy

Effective from April 05, 2024

SHANNON

1. Purpose

The purpose of this policy is to establish comprehensive guidelines and procedures for the backup, storage, and security of sensitive and critical data. This policy aims to ensure the integrity, availability, and confidentiality of data while mitigating risks associated with data loss, unauthorized access, and security breaches.

2. Scope

This policy applies to all employees, consultants, and third-party vendors who have access to Shannon Advisors Private Limited's data, including electronic and physical records. It encompasses data stored on company-owned devices, servers, cloud services, and external storage media.

3. Data Backup Procedures

Data backups must be performed regularly based on the criticality and frequency of data updates.

a) Frequency:

- Daily backups for critical systems and data.

- Weekly backups for less critical data or systems with lower update frequency.

- Monthly or quarterly backups for archival purposes.

b) Backup Schedule: Backup schedule should ensure minimal data loss in case of failures or disasters.

c) Backup Locations: Backups should be stored securely on cloud locations to ensure data availability in various scenarios. Cloud-based backup solutions to be implemented from reputable providers with encryption, access controls, and data redundancy features.

d) Backup Verification: Regular verification and testing of backup integrity and restoration processes must be conducted to ensure the reliability and completeness of backups.

e) Backup Security: All backups should be done on password protected google drive or such other storage as may be notified by the Company.

f) Testing Procedures: Perform regular test restores to verify the integrity and usability of backed-up data.

g) Data Retention: Data Retention should comply with relevant laws and regulations governing data retention and privacy.

h) Review and Update: Regularly review and update data retention policies as needed to reflect changes in regulations, business processes, or data classification.

4. Data Storage Guidelines

a) Access Control: Regularly review and update access permissions as per employees' roles and responsibilities.

b) Storage Security: Ensure that all storage media, including servers, laptops, external drives, and cloud services, comply with company-approved security standards. Implement encryption, access controls, and monitoring mechanisms as necessary.

c) Data Classification: Classify data based on sensitivity levels (e.g., public, internal, confidential, restricted) and apply appropriate security measures, such as access controls, encryption, and data masking, based on the classification.

5. Data Security Measures

a) User Training and Awareness: Conduct regular data security training sessions for employees to educate them about data protection best practices, policies, and procedures. Raise awareness about phishing attacks, social engineering, and other cybersecurity threats.

b) Endpoint Security: Deploy and regularly update endpoint security solutions, including antivirus software, firewalls, and intrusion detection/prevention systems (IDPS), to protect endpoints (e.g., laptops, desktops, mobile devices) from malware and unauthorized access.

6. Compliance and Monitoring

a) Regulatory Compliance: Ensure compliance with relevant data protection laws and regulations applicable to Shannon Advisors Private Limited.

b) Audits and Reviews: Conduct regular internal audits and security assessments to evaluate compliance with this policy, identify potential vulnerabilities, and implement corrective actions. Engage third-party auditors or security experts for independent assessments when necessary.

c) Policy Review: Periodically review and update this data backup, storage, and security policy in response to technological advancements, emerging threats, regulatory changes, and organizational requirements. Seek input from relevant stakeholders during policy revisions.

7. Responsibilities

a) Management: Senior management and IT leadership are responsible for providing necessary resources, support, and oversight to implement and enforce this policy effectively.

b) Employees: All employees, and third parties are responsible for understanding, complying with, and promoting adherence to this policy. Promptly report any security incidents, data breaches, or policy violations to the designated authorities.

8. Enforcement

Violations of this policy, including negligence, intentional misconduct, or non-compliance, may result in disciplinary actions, including but not limited to warnings, suspension, termination of employment/contract, legal consequences, and financial liabilities.

9. Approval and Revision History

This Data Backup, Storage, and Security Policy for Shannon Advisors Private Limited is approved by the Board of Directors and will be reviewed annually or as deemed necessary for updates and improvements.

By adhering to this policy, Shannon Advisors Private Limited aims to protect its valuable data assets, maintain data privacy and confidentiality, mitigate cybersecurity risks, and uphold the trust of clients, partners, and stakeholders.