Backup & Restore Policy

Saturday, June 10, 2023 6:18 PM

1. Purpose: The purpose of this policy is to provide a framework for the backup, recovery, and protection of Beam, Longest and Neff's data, while ensuring business continuity.

2. Scope: This policy applies to all Beam, Longest and Neff employees, contractors, and any other individuals who manage or access company data.

3. Policy:

3.1 Backup Procedures:

3.1.1 Unstructured Data: As we use Nasuni for our unstructured data, we leverage its immutable snapshot feature, which takes snapshots of our data in 5-minute increments. Traditional backup methods are not required for this data.

3.1.2 Structured Data and VMs: Our structured data and VM environment, managed with VMware, are backed up using Veeam. The frequency and retention of backups will be based on the criticality of the data and in accordance with our data retention policy.

3.2 Recovery Procedures: In the event of data loss, recovery procedures must be initiated as soon as possible. Nasuni provides a recovery mechanism via its snapshot feature, and Veeam provides a traditional recovery via an on-premise proxy.

3.3 Testing: Backup and restore procedures must be tested regularly to ensure data can be effectively restored.

3.4 Data Encryption: All backed-up data must be encrypted in transit and at rest to ensure its security.

3.5 Incident Reporting: Any issues or failures related to backups alert necessary IT contacts.

4. Roles and Responsibilities:

4.1 IT Department: The IT department is responsible for managing and executing the backup and restore policy.

4.2 Employees: All employees are responsible for reporting any loss of data to the IT department as soon as they become aware of it.

5. Compliance:

5.1 Compliance Measurement: The IT department will verify compliance to this policy through various methods, including but not limited to, periodic reviews, audits, and feedback.

5.2 Exceptions: Any exception to the policy must be approved by the IT department in advance.

6. Policy Review and Updates:

This policy will be reviewed and updated annually or as required to ensure it remains relevant and effective.

Data Protection Policy

Saturday, June 10, 2023 6:21 PM

1. Purpose: The purpose of this policy is to define standards for the proper use and protection of all company-owned hardware to ensure the confidentiality, integrity, and availability of company data.

2. Scope: This policy applies to all Beam, Longest and Neff employees, contractors, and any other individuals who use or manage company-owned hardware.

3. Policy:

3.1 Hardware Use:

3.1.1 Only authorized personnel may access and use company hardware.

3.1.2 Hardware must be used for business purposes only, and personal use is prohibited unless otherwise specified by management.

3.2 Data Protection:

3.2.1 All company data stored on hardware must be encrypted as per the Storage Encryption Policy.

3.2.2 In the event of hardware malfunction, data should be recovered where possible, and hardware should be repaired or replaced as appropriate.

3.3 Hardware Security:

3.3.1 Hardware should be physically secured to prevent unauthorized access, damage, and theft.

3.3.2 Portable hardware should be securely stored when not in use and never left unattended in an unsecured location.

3.4 Disposal and Decommissioning:

3.4.1 All company data must be securely deleted from hardware before it is disposed of or repurposed.

3.4.2 Hardware should be disposed of in an environmentally responsible manner and in accordance with local laws and regulations.

3.5 Data Sanitization

3.5.1 All hardware assets scheduled for disposal must undergo a thorough data sanitization process to ensure the removal of sensitive and confidential information.

3.5.2 Data sanitization methods should comply with industry best practices and may include secure data wiping using approved software tools, physical destruction, or engaging certified third-party data destruction services.

4. Roles and Responsibilities:

4.1 IT Department: The IT department is responsible for enforcing this policy, managing company hardware, and providing guidance on proper hardware use and data protection.

4.2 Users: Users are responsible for using hardware appropriately, protecting company data, and reporting any hardware loss, theft, damage, or unauthorized access.

5. Compliance:

5.1 Compliance Measurement: The IT department will verify compliance to this policy through various methods, including but not limited to, periodic reviews, audits, and feedback to the policy owner.

5.2 Exceptions: Any exception to the policy must be approved by the IT department in advance.

5.3 Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Policy Review and Updates:

This policy will be reviewed and updated annually or as required to ensure it remains relevant and effective.