BWEvents LLC
Data purge, delete, destruction Policy

Revision History

Version	Date	Author	Description of changes
1.0	02/01/2022	Satish Baniya	Initial Release
1.1	05/01/2023	Satish Baniya	Review and updates
1.2	12/01/2023	Satish Baniya	Review and updates

1. Purpose:

The purpose of this policy is to establish guidelines for the timely and secure purging, destruction, or rendering of unreadable critical data that is no longer needed by BWEvents Tech. This policy aims to protect sensitive information from unauthorized access and reduce data retention risks in compliance with relevant laws, regulations, and industry best practices.

2. Scope:

This policy applies to all employees, contractors, and third-party personnel who handle critical data within BWEvents Tech's information systems and databases.

3. Policy:

3.1. Data Retention Period:

1. Critical data shall only be retained for the duration necessary to fulfill business, legal, and regulatory requirements.
2. BWEvents Tech will establish clear data retention periods based on the sensitivity of the data and applicable laws and regulations.

3.2. Identification of Data for Purging or Destruction:

1. BWEvents Tech shall conduct periodic reviews to identify critical data that is no longer required for business purposes or legal obligations.
2. Data owners or designated personnel will be responsible for assessing the necessity of retaining specific datasets.

3.3. Purging, Destruction, or Rendering Data Unreadable:

1. Data that has met its retention period and is no longer required shall be purged, deleted, or made unreadable using secure data disposal methods.
2. The method of data destruction will depend on the data type, format, and medium and may include physical destruction or secure wiping techniques.

3.4. Secure Data Disposal:

1. The data purging and destruction process must adhere to industry best practices and comply with applicable data protection and privacy laws.
2. The use of data shredders, degaussing equipment, or software-based data wiping tools may be employed to ensure secure disposal.

3.5. Documentation and Recordkeeping:
1. BWEvents Tech shall maintain proper documentation of data purging and destruction activities.
2. Records must include details of the data purged, the date of disposal, the method used, and the personnel responsible for the process.

3.6. Data Backup Considerations:
1. Before data is purged or destroyed, appropriate data backups, if required, must be created to meet business continuity needs and legal requirements.
2. Backup copies should be stored securely and in accordance with data retention policies.

3.7. Training and Awareness:
1. Employees and authorized users handling critical data must receive training on the data purging and destruction procedures and their significance.
2. Regular awareness programs shall be conducted to reinforce the importance of securely disposing of data.

4. Responsibilities:

4.1. Data Owners or Designated Personnel:
1. Data owners or designated personnel are responsible for identifying data for purging or destruction based on the established retention periods.
2. They must ensure that critical data is disposed of in compliance with this policy.

4.2. IT Department:
1. The IT department is responsible for implementing data purging and destruction procedures and providing technical support as needed.
2. They must ensure that data is purged or destroyed securely and that proper documentation is maintained.

4.3. Employees and Authorized Users:
1. Employees and authorized users must comply with this policy and report any data retention practices that are contrary to this policy.

5. Compliance and Enforcement:
Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

6. External Data Destruction Requests:

6.1. Client Initiated Data Destruction:

Client Request Process:
- Clients seeking data destruction for information handled by BWEvents Tech must submit a written request to their designated project manager via an email.
- The written request should clearly specify the data to be purged or destroyed, the reasons for the request, and any applicable deadlines.

Project Manager Responsibilities:
- The designated project manager will review and validate the client's request for data destruction.
- If the request aligns with the agreed-upon terms and conditions, the project manager will coordinate with internal stakeholders to initiate the data destruction process.

Verification and Authorization:
- The project manager is responsible for verifying the authenticity of the client's request and obtaining any necessary authorizations before proceeding with the data destruction.

Communication:
- The project manager will maintain clear and documented communication with the client throughout the data destruction process, providing updates on the status and any relevant information.

6.2. Data Destruction Process:

Secure Handling:
The IT department will oversee the secure handling and destruction of data as per the client's request, ensuring compliance with all applicable legal and regulatory requirements.

Documentation:
Proper documentation of the data destruction process will be maintained, including details of the client request, the data purged, the method used, and the personnel involved.

Notification to Client:
Upon completion of the data destruction, the project manager will notify the client, confirming the successful execution of the request.

6.3. Compliance and Recordkeeping:

Record Retention:
Records of client-initiated data destruction activities will be retained in accordance with the data retention policies.

7. Review and Amendment

This policy will be reviewed regularly to ensure its continued relevance and alignment with evolving data protection requirements and industry standards.