BWEvents LLC
Confidential Data 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. Purpose:
The Confidential Data Policy of BWEvents establishes guidelines and procedures to ensure the proper handling, protection, and retention of confidential information. This policy aims to safeguard sensitive data from unauthorized access, disclosure, erasure, or destruction.

2. Scope:
This policy applies to all employees, contractors, vendors, and third-party service providers who have access to confidential information in the course of their work at BWEvents.

3. Defining, Identifying, and Designating Confidential Information:
3.1. Definition:
Confidential information includes any data or materials that, if disclosed, could cause harm to BWEvents, its clients, employees, or partners, or violate privacy regulations.

3.2. Identification:
BWEvents will perform a thorough data classification process to identify and categorize information based on its sensitivity and criticality. The classification will include levels such as Public, Internal Use Only, and Confidential.

3.3. Designation:
Confidential information will be explicitly labeled or marked with appropriate headers, footers, or watermarks to indicate its confidential nature.

4. Storing Confidential Information:
4.1. Secure Storage:
Confidential information must be stored in designated secure locations, such as password-protected folders, encrypted databases, or physical locked cabinets.

4.2. Access Control:
Access to confidential data will be restricted on a need-to-know basis. Only authorized personnel with legitimate business reasons will be granted access.

4.3. Portable Devices:

Confidential data stored on portable devices, such as laptops, smartphones, or external drives, must be encrypted and password-protected.

5. Protecting Confidential Information from Erasure or Destruction:

5.1. Data Backups:

Regular backups of confidential data will be performed and stored securely to ensure data integrity and availability in case of data loss or system failures.

5.2. Data Retention:

Confidential data will be retained for only as long as necessary to achieve the purpose for which it was collected and processed. After the retention period expires, data will be securely erased or destroyed following approved procedures.

5.3. Disposal:

When disposing of physical or electronic media containing confidential information, a secure disposal process will be followed to prevent unauthorized access.

6. Access Monitoring and Auditing:

BWEvents will implement access monitoring and auditing mechanisms to track and review access to confidential data. Logs will be periodically reviewed for suspicious activities or unauthorized access.

7. Training and Awareness:

All employees and authorized users will receive training and awareness programs to understand the importance of safeguarding confidential information and the procedures to be followed.

8. Reporting Security Incidents:

Any suspected or actual security incidents related to confidential data must be reported immediately to the IT Security team or designated personnel for investigation and response.

9. Compliance:

All employees and stakeholders with access to confidential data are required to comply with this policy. Non-compliance may result in disciplinary actions.

10. Review and Updates:

This Confidential Data Policy will be reviewed periodically to ensure its relevance and effectiveness. Any necessary updates or modifications will be implemented promptly.