

BW Events LLC
Access Review Policy

Revision History

Version	Date	Author	Description of changes
1.0	08/01/2023	Satish Baniya	Initial Release

1. Purpose:

The purpose of this Access Review Policy is to ensure that access rights to applications and environments within BW Events are regularly reviewed and validated to maintain the integrity, confidentiality, and availability of sensitive data.

2. Scope:

This policy applies to all applications and environments, including production, staging, and development, within the BW Events infrastructure.

3. Policy Statement:

Access to applications and environments must be reviewed periodically to confirm that users have the appropriate level of access required for their roles and responsibilities. This policy outlines the procedures for conducting access reviews and the responsibilities of individuals involved.

4. Access Review Process:

4.1. Frequency:

Access reviews will be conducted at least annually to ensure that access rights are aligned with the current roles and responsibilities of users.

4.2. Responsible Parties:

- Access reviews will be led by the DevOps team in coordination with the IT Security Team.
- Application owners and department heads are responsible for validating and confirming access rights for their respective areas.

4.3. Access Review Steps:

- Identify a list of users with access rights to applications and environments.
- Application owners and department heads review and confirm the access rights for individuals within their areas.
- The IT Security Team verifies the reviews conducted by the application owners and department heads.
- Any discrepancies or unauthorized access is reported and addressed promptly.

5. Remediation:

- Upon identification of discrepancies or unauthorized access, corrective actions must be taken promptly.
- Remediation may include adjusting access rights, conducting additional training, or initiating disciplinary actions as per the BW Events policies.

6. Documentation:

- Access reviews and their outcomes will be documented and maintained for audit purposes.
- Records will include details of individuals involved in the review, access changes made, and the rationale behind those changes.

7. Notification:

- Users will be notified in advance of the upcoming access review to ensure their availability for validation.
- Any access changes resulting from the review will be communicated to the affected users and their respective supervisors.

8. Compliance:

- The IT Security Team will conduct periodic audits to ensure compliance with this Access Review Policy.

9. Review and Revision:

- This policy will be reviewed [Specify Frequency - e.g., annually] and updated as needed to reflect changes in the organization's structure, technology, or security requirements.

10. Approval:

- This Access Review Policy is approved by [Specify Approving Authority] and will be effective as of [Specify Effective Date].

11. Distribution:

- This policy will be distributed to all relevant parties, including application owners, department heads, and IT personnel.