

# Access Control Policy

## BW Events LLC

### Revision History

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

### **1. Purpose**

The purpose of this Access Control Policy is to define the principles, guidelines, and procedures for controlling physical and logical access to information and associated assets at BW Events Tech. This policy aims to safeguard the confidentiality, integrity, and availability of data while ensuring compliance with business and information security requirements.

### **2. Scope**

This policy applies to all employees, contractors, third-party users, and any other individuals granted access to BW Events Tech's information systems and assets.

### **3. Policy Statement**

BW Events Tech is committed to enforcing strict access control measures for the protection of information and associated assets. Access control rules, both for physical and logical access, shall be established and implemented in alignment with business and information security requirements.

### **4. Access Control Principles**

#### **4.1. Least Privilege**

Access to information and assets shall be granted based on the principle of least privilege. Users will be provided with the minimum level of access required to perform their job responsibilities.

#### **4.2. Need-to-Know**

Access shall be granted on a "need-to-know" basis. Users will only be provided with information that is necessary for them to fulfill their roles and responsibilities.

#### **4.3. Role-Based Access Control**

Access permissions will be assigned based on job roles and responsibilities. Users' access rights will correspond to their designated roles.

#### **4.4. Access Revocation**

Access rights shall be revoked promptly when no longer required due to job changes or project completion. The access revocation process will be well-defined and implemented.

#### **4.5. Authentication and Authorization**

- Users shall be required to authenticate themselves using secure and appropriate methods (e.g., passwords, multi-factor authentication) before gaining access.
- Authorization mechanisms will be in place to verify users' access rights.

#### **4.6. Logging and Monitoring**

- All access activities, both physical and logical, will be logged and regularly reviewed.
- Monitoring of access logs will be performed to detect and respond to suspicious activities.

### **5. Physical Access Control**

Physical access controls do not apply to BW Events' fully remote mailing address. All corporate operations, ISMS management, and software development activities are conducted remotely.

### **6. Logical Access Control**

#### **6.1. User Account Management**

- User accounts will be created, modified, and disabled following established procedures
  - Request is submitted through email
  - Request is approved through email
  - Once a request is approved, an account is created and shared with the account holder.
- Access to systems and data will be controlled through user account management.

#### **6.2. Password Security**

- Strong password policies will be enforced, requiring users to create and maintain secure passwords.
- Password changes and resets will follow established rules.

#### **6.3. Access Reviews**

Regular access reviews and audits will be conducted to ensure that access rights are consistent with business needs and responsibilities.

## **7. Compliance**

Failure to comply with this Access Control Policy may result in disciplinary action in accordance with BW Events Tech's policies and procedures.

## **8. Review and Updates**

This Access Control Policy will be reviewed periodically to ensure its relevance and alignment with business and information security requirements. Any necessary updates or modifications to the policy shall be implemented promptly.