ACCESS CONTROLS POLICY

Version: V2
Date: April 8, 2022

SCOPE

This policy will apply to the Joint Industry Board of the Electrical Industry (JIBEI) and all affiliates, including JIB Medical, P.C. This policy applies to all employees, consultants and contractors that connect to servers, applications or network devices that contain or transmit JIBEI, and their affiliates, Confidential and/or Restricted Data, per the Data Classification and Governance Policy.

PURPOSE

Access Controls are designed to protect the confidentiality, integrity, and availability of the JIBEI networks, systems, and applications. Without proper access controls, undesired or unauthorized access could occur resulting in breach of PHI and/or PII data, financial loss, reputational damage, or failure to meet HIPAA and/or other requirements.

POLICY

Access to systems containing PHI, PII, Financial or Confidential information will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. All access requests for these systems must be entered into the JIBEI User Provisioning application, or otherwise approved by the Director of Administration or the CTO. Each user shall be granted access using a unique ID or account. Users must adhere to security guidelines as outlined in the JIBEI Information Security Policy.

Access will be granted based on:

- **Least Privilege:** Users will only be granted access to data for the purpose of executing their responsibilities and duties. Right to access the above data shall not be granted unless there is a legitimate business or medical need.
- **Segregation of Duties:** Users should not be able to grant themselves rights. The IT department is responsible for provisioning access to the network/Active Directory and organization wide JIBEI applications. Administrators must adhere to the guidelines stated in the Privileged User Access Guidelines of the IT Controls Policy & Procedures. Individual departments that utilize department-

specific applications shall designate someone to provision access to that application in accordance with separation of duties.

- **Role Based Access:** Users will be assigned access rights based on functional roles they assume while conducting JIBEI business.
- **Removal of Access:** Access must be promptly removed upon the user's termination or other separation from JIBEI. When an employee transfers, the [new] manager must request the access needed for the new position in the User Provisioning system and the IT department will remove all prior access not re-requested for the new position.
- **Standards and Guidelines for Passwords, Remote Access** and other security guidelines are outlined in the Information Security Policy.
- **Account Types:**
    - Default Accounts – shall be disabled, removed, or renamed. All default passwords must be changed.
    - Service Accounts – background accounts necessary for applications to run and are not used by users or administrators to log in. Where possible, service accounts should be configured to prevent interactive login.
    - Generic Accounts – accounts that are used by multiple people lack accountability and shall not be used. Resource accounts that to not have a login, such as group mailboxes, do not utilize the resource account for authentication and are not considered generic accounts.
    - Privileged Accounts – Administrator and other privileged accounts shall be created only where needed to manage the system and must adhere to the Privileged User Access Guidelines of the IT Controls Policy & Procedures. Privileged Accounts require multifactor authentication.
- **Multi-Factor Authentication:**
    - Multi-Factor Authentication (MFA) is adding another factor besides a password for authentication, usually something you know or something you have. MFA is required for access in the following circumstances:
        - Remote access
        - Privileged user access
        - RDP access to servers and network devices
        - Access to networking devices

REFERENCES

Information Security Policy
IT Controls Policy & Procedures (including User Provisioning and Guidelines for Privileged Users sections)
Data Classification and Governance Policy

REVISION HISTORY

Revision Tracking		
Version #	Revision Date	Revision Notes
V1	5/31/2021	Initial
V2	4/8/2022	Added Multi Factor Authentication