Access Control Policy

Policy Owner: Georgia Donmoyer

Effective Date: January 1, 2023

Purpose

To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

Scope

All Mesh Intelligent Technologies, Inc. information systems that process, store, or transmit confidential data as defined in the Mesh Intelligent Technologies, Inc. Data Management Policy. This policy applies to all employees of Mesh Intelligent Technologies, Inc. and to all external parties with access to Mesh Intelligent Technologies, Inc. networks and system resources.

Policy

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

Business Requirements of Access Control

Access Control Policy

Mesh Intelligent Technologies, Inc. shall determine the type and level of access granted to individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by Mesh Intelligent Technologies, Inc.'s business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited.

Mesh Intelligent Technologies, Inc.'s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production infrastructure shall use Multi-Factor Authentication (MFA).

Access to Networks and Network Services

The following security standards shall govern access to Mesh Intelligent Technologies, Inc. networks and network services:

- Technical access to Mesh Intelligent Technologies, Inc. networks must be formally documented including the standard role or approver, grantor, and date
- Only authorized Mesh Intelligent Technologies, Inc. employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the Mesh Intelligent Technologies, Inc. production networks and resources
- Mesh Intelligent Technologies, Inc. guests may be granted access to guest networks after registering with office staff without a documented request
- Remote connections to production systems and networks must be encrypted

Customer Access Management

When configuring cross-account access using AWS IAM roles, you must use a value you generate for the external ID, instead of one provided by the customer, to ensure the integrity of the cross account role configuration. A partner-generated external ID ensures that malicious parties cannot impersonate a customer's configuration and enforces uniqueness and format consistency across all customers.

The external IDs used must be unique across all customers. Re-using external IDs for different customers does not solve the confused deputy problem and runs the risk of customer A being able to view data of customer B by using the role ARN of customer B along with the external ID of customer B.

Customers must not be able to set or influence external IDs. When the external ID is editable, it is possible for one customer to impersonate the configuration of another.

User Access Management

Mesh Intelligent Technologies, Inc. requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed. If a password is compromised or suspected of compromise it must be changed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a documented request from authorized parties. User provisioning requests must include approval from data owners or Mesh Intelligent Technologies, Inc. management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any Mesh Intelligent Technologies, Inc. security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions.

User IDs shall be promptly disabled or removed when users leave the organization or contract work ends in accordance with SLAs. User IDs shall not be re-used.

User Access Provisioning

- New employees and/or contractors are not to be granted access to any Mesh Intelligent Technologies, Inc. production systems until after they have completed all HR on-boarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and acknowledgement of Mesh Intelligent Technologies, Inc.'s information security policy
- Access should be restricted to only what is necessary to perform job duties
- No access may be granted earlier than official employee start date
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system or data owner or management
- Records of all permission and privilege changes shall be maintained for no less than one year

Management of Privileged Access

Granting of administrative rights shall be strictly controlled, and requires approval from the asset owner.

User Access Reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.

Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

Removal & Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

Access Provisioning, Deprovisioning, and Change Procedure

The Access Management Procedure for Mesh Intelligent Technologies, Inc. systems can be found in Appendix A to this policy.

Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Mesh Intelligent Technologies, Inc. assets. When provisioning access, care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered when determining access levels for individuals and groups.

User Responsibility for the Management of Secret Authentication Information

Control and management of individual user passwords is the responsibility of all Mesh Intelligent Technologies, Inc. personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

Password Policy

Where feasible, passwords for confidential systems shall be configured for at least:

- Eight (8) or more characters, one upper case, one number
- Passwords shall be set to lock out after 6 failed attempts
- Passwords shall expire after days
- Initial passwords must be set to a unique value and changed after first log in
- For manual password resets, a user's identity must be verified prior to changing passwords
- Do not limit the permitted characters that can be used
- Do not limit the length of the password to anything below 64 characters
- Do not use secret questions (place of birth, etc) as a sole password reset requirement
- Require email verification of a password change request
- Require the current password in addition to the new password during password change
- Verify newly created passwords against common passwords lists or leaked passwords

databases
- Check existing user passwords for compromise regularly
- Store passwords in a hashed and salted format using a memory-hard or CPU-hard one-way hash function
- Enforce appropriate account lockout and brute-force protection on account access

System and Application Access

Information Access Restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to Mesh Intelligent Technologies, Inc. policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Mesh Intelligent Technologies, Inc. systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, and Simple Network Management Protocol (SNMP) community strings where feasible.

Secure Log-on Procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

Password Management System

Systems for managing passwords should be interactive and assist Mesh Intelligent Technologies, Inc. personnel in maintaining password standards by enforcing password strength criteria including minimum length, and password complexity where feasible.

All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption.

Use of Privileged Utility Programs

Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required. Systems are to maintain logs of all use of system utilities or alteration of system configurations. Extraneous system utilities or other privileged programs are to be removed or disabled as part of the system build and configuration process.

Management approval is required prior to the installation or use of any ad hoc or third-party system utilities.

Access to Program Source Code

Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect Mesh Intelligent Technologies, Inc. intellectual property.

All access to source code shall be based on business need and must be logged for review and audit.

Exceptions

Requests for an exception to this Policy must be submitted to the IT Manager for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the IT Manager. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	14-Feb-2023	First Version	Georgia Donmoyer	Tsavo Knott

APPENDIX A - Access Management Procedure

At the completion of the onboarding process, HR will send an email that will generate a series of service tickets for access.

IT will provision access for all company-wide systems as well as engineering systems for the Members of Technical Staff (MTS) group.

Additional access, beyond standard pre-approved access, must be requested and approved by a manager or system owner.

APPENDIX B - Access Matrix

Role	Email	Google Wrkspc	Gusto	CRM	App	Infrastructure	Version Control	Build System	Vuln Scanner
Employee	x	x	x		x				
Engineer	x	x	x		x	x	x	x	
Engineer Sprvs	x	x	x		x	x	x	x	x
Sales & Business Dev	x	x	x	x	x				
Growth & Marketing	x	x	x		x				