**Security Policy:**

**Access Control Policy**

This policy / procedure complies with the requirements of the ISO 27001:2013 International Standard

Annex A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.5, A.11.1.5, A.13.1.1, A.13.1.2

[**Company Name]**

[Address]

[City, State Zip]

**1. Purpose**

The purpose of this document is to define the policy and procedure requirements governing access to various systems, equipment, facilities and information, based on business and security requirements for [Company Name].

**2. Scope**

This policy applies to all [Company Name] owned and customer-owned information assets and all managed facilities and, networks, systems, and technology assets that store, process or transmit information within the scope of the Information Security Management System (ISMS).

**3. Policy (A.9.1.1, 9.1.2)**

It is the policy of [Company Name] that the principle of *least* *privilege* shall apply to the provisioning of all access rights. That is, access to information, networks, systems, technologies, and facilities is provided to employees, subcontractors, supplier partners, customers (collectively **users**) only to a level and scope necessary to perform assigned duties and/or to fulfill contracted services.

Users are always identified, registered, and their access privileges assigned, managed, and rescinded, as described in the HR Security Policy, and this Access Control Policy. Regardless of the specific access privileges that may be assigned, all users are required to comply with the requirements of the Information Classification Policy and the Information Handling and Labeling Policy found in the ISMS Plan document.

**4. Responsibilities**

Roles and responsibilities regarding specific access assignments are as follows.

* Managers / supervisors are responsible for defining roles and requesting role-based access privileges for users under their oversite.
* Information, system, and technology Asset Owners are responsible for reviewing and approving requests for access to assets they own.
* Deliberate circumvention of this policy constitutes a breach of security and, upon detection, should be Immediately reported in accordance with the Incident Management Policy and Procedure.

**5. PROCEDURES**

Implementation note: the following requirements may be met using any combination of automated and/or manual systems as long as compliance to the requirements can be clearly evidenced by the system(s).

# User Registration (A.9.2.1)

All internal and external users of information systems within the scope of the ISMS are formally registered as users as follows:

* A unique user ID is assigned, one per user. (Exceptions to this rule including assignment of group user id’s to multiple users require sign-off by the [**Insert function or title here**].
* Systems to which the user ID will be granted privileges and access are explicitly identified. (See Privilege Management below.)
* Users are immediately removed from registration when they depart the organization (see HR Security Policy).
* Registrations are reviewed at least annually to assure there are no redundant, or expired registrants.

# Access / Privilege Management and Provisioning (A9.2.2, A.9.2.3, A.9.2.4, A.9.4.1, A.9.4.5)

Allocation and provisioning of access rights is controlled as follows:

* Only registered users are assigned access rights.
* Access rights to specific ISMS in-scope facilities, systems or assets are identified by the manager or individual with supervisory over-site of the registered user.
* Access rights are granted on an as-needed basis and approved by the supervisor and the owner/administrator of the system(s), in keeping with the least-privilege principle. Factors considered in the granting of access rights include:
	+ Information / data that for which the user’s business role or job function requires read, edit, or delete access.
	+ Systems that provide access to that data.
* Privileged access rights (e.g., administrator level) are assigned only on an as-needed basis and require the additional approval of the [**Insert function or title here**]. Privileged access requires assignment of a unique id if the assignee is already registered as a user.
* Access to program source code is assigned only on as as-needed basis and requires the additional approval of the [**Insert function or title here**] and the [**Insert function or title here**]. Authorizations are recorded. No access rights are granted until the authorization process is complete.
* Provisioning of access rights may include keys, identification badges, security lock devices, or access codes for physical facilities, or login credentials to systems or technology assets.
* Users are required to sign a statement of confidentiality, as part of the terms and conditions of employment, for privileged (e.g., administrator) access rights. (See HR Security Policy)
* Initial login credentials are temporary – all systems require password change on first login.
* User-level access rights must be renewed at least annually to assure ongoing alignment with business need.
* Privileged access rights are renewed at least every six months to assure ongoing alignment with job responsibilities.
* Accidental or intentional circumvention of the above process constitutes a security breach that must be immediately raised as a security incident in accordance with the Incident Management Procedure.

# Review and Management of Access Rights (A.9.2.5, A.9.2.6, A.8.1.4)

Users’ access rights are reviewed at least annually.

* User’s access rights are reviewed whenever there is a change in the status of the user. Examples of change include promotion, demotion, transfer, or termination of the relationship. (See HR Security Policy).
* User’s access rights are reviewed whenever there is a change in the status of a facility or system to which the user has been granted access. Examples include facility lock changes, major system upgrades, system replacement, or a change in the use and purpose of the system within the business.
* Changes in access provisions based on the review include both granting of new and appropriate access and rescinding of prior access that is no longer justified by business need.
* Removal of access rights includes return of any facility keys, identification badges, security lock devices, and removal of accounts from systems.
* A notice of termination automatically triggers a review of access rights for the user, and immediate reduction or removal of such rights depending on the reason for termination, the nature of the user relationship to the business, and the assessed information security risk. (See HR Security Policy)
* Upon termination of the business relationship with [Company Name], all previously issued physical and electronic assets must be returned to [Company Name].
* Changes to user access and privileged access accounts are logged.

# Network Access Control (A.13.1.1, A.13.1.2)

Network access is controlled as follows.

* Internal access to the network and attached resources is controlled in accordance with the User Registration and Access and Privilege Management process noted above.
* External access to the network is controlled in accordance with the User Registration and Access and Privilege Management process noted above. All external access requires use of the Virtual Private Network (encrypted) over any public communications channels.
* Network logs of access are maintained.

# Physical Access control (A.11.1.1, A.11.1.2, A.11.1.5)

The [Company Name] facilities subject to these policy requirements are located at:

* [site 1 address]
* [site 2 address]
* [site 3 address]

Perimeter Security is managed as follows:

* <describe physical security measures that may be in place including electronic surveillance, keyed or pass-code locks, biometric locks, intrusion detection systems, etc. – as appropriate to the vulnerabilities and threats relevant to your business model and information security risks. For example,:>
	+ Security guards patrol the Building 24 x 7
	+ Staff verify individual access authorizations before granting access to the office suite.
	+ Control entry to the office suite containing the system using physical access devices.
	+ Secure key card access, combinations and other physical access devices.
	+ Change combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

# Login and Password Management (A.9.3.1,A.9.4.2, A.9.4.3)

Authentication Information (login credentials) are protected as follows:

* Login credentials are confidential and are not divulged to anyone by the user. No exceptions.
* Login credentials are not written down, stored in electronic files, or other media.
* The only acceptable login credential storage is within the <name of credential management application, e.g., LastPass, if one is in place.> or in an approved secure credential repository.

Login procedures implemented on all business applications and customer-facing applications are implemented as follows:

* No help messages are available that would aid in an unauthorized login attempt.
* Log-in information is validated only on completion of all login inputs.
* User is locked out after a set number of unsuccessful login attempts.
* Passwords are not displayed during entry (unless the user enables “display password”).
* Passwords are not transmitted in clear text.
* Inactive / uncompleted login attempts terminate inactive sessions after a defined period of inactivity.

Passwords are managed as follows:

* Each user ID is associated with only one password.
* Users may select and change their own passwords.
* Rules enforcing strong passwords are enforced automatically in all systems.
* Passwords are required to be reset immediately upon first login to systems.
* Periodic password changes are enforced by the systems.
* Reuse of previous passwords is automatically prevented.
* Passwords do not display on the screen during entry.
* Passwords are only entered over encrypted links.

**6. ACCESS CONTROL records**

* User Registration Log
* Access Provisioning Records
* Access Review Records

**7. reference documents**

* Information Classification Policy
* Information Handling Policy
* Incident Management Policy/Procedure
* HR Security Policy