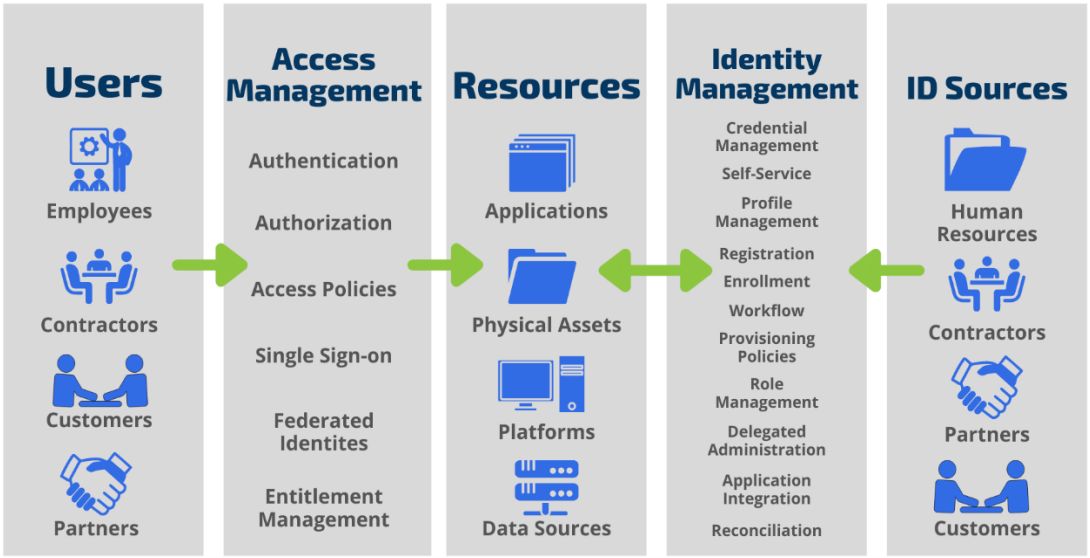
Identity and Access Management Policy



Identity and Access Management Policy, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Information Security Committee
Last Review Date: April 2024

Identity and Access Management Policy

Purpose

The purpose of the (Company) Identity and Access Management Policy is to establish the requirements necessary to ensure that access to and use of (Company) Information Resources is managed in accordance with business requirements, information security requirements, and other (Company) policies and procedures.

Audience

The (Company) Identity and Access Management Policy applies to individuals who are responsible for managing (Company) Information Resource access, and those granted access privileges, including special access privileges, to any (Company) Information Resource.

Contents

Policy

Access Control

- Access to (Company) Information Resources must be justified by a legitimate business requirement prior to approval.
- Where multi-factor authentication is employed, user identification must be verified in person before access is granted.
- (Company) Information Resources must have corresponding ownership responsibilities identified and documented.
- Access to confidential information is based on a "need to know".
- Confidential data access must be logged.
- Access to the (Company) network must include a secure log-on procedure.
- Workstations and laptops must force an automatic lock-out after a pre-determined period of inactivity.
- Documented user access rights and privileges to Information Resources must be included in disaster recovery plans, whenever such data is not included in backups.

Account Management

- All personnel must sign the (Company) Information Security Policy Acknowledgement before access is granted to an account or (Company) Information Resources.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.
- Information Resource owners are responsible for the approval of all access requests.
- User accounts and access rights for all (Company) Information Resources must be reviewed and reconciled at least annually, and actions must be documented.
- All accounts must be uniquely identifiable using the username assigned by (Company) IT and include verification that redundant user IDs are not used.
- All accounts, including default accounts, must have a password expiration that complies with the (Company) Authentication Standard.
- Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege".
- Whenever possible, access to Information Resources should be granted to user groups, not granted directly to individual accounts.
- Shared accounts must not be used. Where shared accounts are required, their use must be documented and approved by the Information Resource owner and use compensating controls to ensure non-repudiation.
- User account set up for third-party cloud computing applications used for sharing, storing and/or transferring (Company) confidential or internal information must be approved by the resource owner and documented.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Any accounts that have not been accessed within a defined period of time will be disabled.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- System Administrators or other designated personnel:
    - Are responsible for modifying and/or removing the accounts of individuals that change roles with (Company) or are separated from their relationship with (Company).
    - Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
    - Must have a documented process for periodically reviewing existing accounts for validity.
    - Are subject to independent audit review.
    - Must provide a list of accounts for the systems they administer when requested by authorized (Company) IT management personnel.
    - Must cooperate with authorized (Company) Information Security personnel investigating security incidents at the direction of (Company) executive management.

Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Administrative/Special access accounts must employ multi-factor authentication for all account logins.

- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves (Company) altogether.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- Special access accounts for internal or external audit, software development, software installation, or other defined need, must be administered according the (Company) Authentication Standard.

Authentication

- All passwords, including initial and/or temporary passwords, must be constructed according to the (Company) Authentication Standard,
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (i.e. security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual, and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated and unnecessary default accounts removed or disabled before installing a system on the network.
- User account passwords must not be divulged to anyone. (Company) support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with (Company), if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the (Company) Authentication Standard for the sake of ease of use.
- Users should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the (Company) IT Management.
- If a password management system is employed, it must be used in compliance with the (Company) Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off of the device.
- (Company) IT Support password change procedures must include the following:
    - authenticate the user to the helpdesk before changing password
    - change to a strong password
    - require the user to change password at first login.
- In the event that a user's password is compromised or discovered, the password must be immediately changed, and the security incident reported to (Company) IT support.

Remote Access

- All remote access connections to the (Company) networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
- Remote users may connect to the (Company) networks only after formal approval by the requestor's manager or (Company) Management.
- The ability to print or copy confidential information remotely must be disabled.
- Users granted remote access privileges must be given remote access instructions and responsibilities.
- Remote access to Information Resources must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the (Company) network unless approved in advance by (Company) IT management.
- Non-(Company) computer systems that require network connectivity must conform to all applicable (Company) IT standards and must not be connected without prior written authorization from IT Management.
- Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.

Vendor Access

- Vendor access must be uniquely identifiable, provide non-repudiation, and comply with all existing (Company) policies.
- External vendor access activity must be monitored.
- All vendor maintenance equipment on the (Company) network that connects to the outside world via the network, telephone line, or leased line, and all (Company) Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 6, 7, 8, 9, 12, 15
- NIST CSF: PR.AC, PR.IP, PR.MA, PR.PT, DE.CM
- Information Classification and Management Policy
- Continuity and Recovery Policy
- Information Security Policy Acknowledgement

Waivers

Waivers from certain policy provisions may be sought following the (Company) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	August 2020		Manager	Document Origination