Purpose: The purpose of this policy is to ensure that access to company resources is authorized and managed effectively, and that modifications to access rights are performed in a controlled and secure manner. This policy also establishes the requirements for Identity Access Management (IAM) to ensure that individuals are granted appropriate levels of access to company resources based on their job responsibilities and needs.

Scope: This policy applies to all employees, contractors, vendors, and other third parties who require access to company resources, including but not limited to data, systems, applications, and networks.

Policy:

Access Authorization:

1. Access to company resources must be authorized in accordance with the principle of least privilege, where access is granted based on the minimum level required to perform job responsibilities and tasks.
2. Access to company resources must be granted based on business need and must be approved by the relevant business owner or manager.
3. Access to sensitive and confidential information must be granted on a need-to-know basis and must be approved by the relevant data owner or manager.
4. Access to company resources must be reviewed and reauthorized periodically, at least annually, to ensure that access is still required and appropriate.

Modification of Access Rights:

1. Changes to access rights must be made in accordance with the principle of least privilege and must be approved by the relevant business owner or manager.
2. Changes to access rights must be logged and tracked to ensure accountability and auditability.
3. Changes to access rights must be communicated to the affected individuals and the relevant data owner or manager.
4. Changes to access rights must be performed in a controlled and secure manner to prevent unauthorized access or modifications.

Identity Access Management:

1. IAM must be used to manage user identities and access rights to company resources.
2. IAM must include processes for creating, modifying, and deleting user accounts and access rights.
3. IAM must use strong authentication mechanisms, such as multi-factor authentication, to verify user identities.
4. IAM must enforce password policies, such as complexity requirements and password expiration, to ensure that user accounts are secure.
5. IAM must provide centralized logging and reporting capabilities to enable auditing and monitoring of access rights and user activities.

Enforcement:

1. Violations of this policy may result in disciplinary action, up to and including termination of employment or contractual agreement.
2. This policy is subject to periodic review and may be updated or revised as necessary to reflect changes in technology, business practices, and regulatory requirements.
3. Employees, contractors, vendors, and other third parties must adhere to this policy and report any suspected violations to the appropriate manager or the company's information security team.

References:

1. ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements.
2. NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations.