ISA Inc. Active Directory Policy and Standards

1. Introduction

Active Directory (AD) is a critical component of ISA Inc.'s IT infrastructure. It is used for user and computer authentication, authorization, and policy enforcement. This document outlines the policies and standards for managing AD to ensure the security, reliability, and efficiency of the system.

2. Scope

This policy applies to all employees, contractors, and third parties who have access to or manage the Active Directory infrastructure at ISA Inc. It covers all aspects of AD, including design, implementation, management, and security.

3. Objectives

- **Security:** Ensure the integrity, confidentiality, and availability of the AD environment.
- **Compliance:** Adhere to industry standards and regulatory requirements.
- **Efficiency:** Optimize AD management processes to reduce administrative overhead.
- **Consistency:** Maintain a uniform and standardized AD environment.

4. Governance

The AD governance team, comprising senior IT managers, security officers, and system administrators, will oversee the implementation and enforcement of this policy. Regular audits and reviews will be conducted to ensure compliance and address any issues.

5. Design and Architecture

5.1. Domain Structure

- **Single Forest, Single Domain:** ISA Inc. will maintain a single forest, single domain structure to simplify management and enhance security.
- **Naming Conventions:** Use a consistent naming convention for domains, OUs, and objects. For example, isa.local for the domain and OU=Users, DC=isa, DC=local for the user OU.

5.2. Organizational Units (OUs)

- **OU Hierarchy:** Organize OUs based on business units, departments, and roles to facilitate delegated administration and policy enforcement.
- **Standard Naming:** Use a standard naming convention for OUs, such as OU=Sales, OU=Departments, DC=isa, DC=local.

5.3. Sites and Services

- **Site Configuration:** Configure AD sites to reflect ISA Inc.'s physical network topology, enhancing replication efficiency.
- **Subnet Mapping:** Ensure all IP subnets are mapped to the correct AD sites.

6. User and Group Management

6.1. User Accounts

- **Account Creation:** Follow a standardized process for creating user accounts, including unique usernames, initial passwords, and required attributes.
- **Naming Convention:** Use a consistent naming convention, such as firstname.lastname.

- **Account Lifecycle:** Implement procedures for account provisioning, de-provisioning, and modification.
- **Password Policies:** Enforce strong password policies, including complexity requirements, expiration periods, and history checks.

6.2. Group Management

- **Group Types:** Use security groups for permissions and distribution groups for email purposes.
- **Group Scopes:** Use global groups for user accounts, domain local groups for permissions, and universal groups for cross-domain resources.
- **Naming Convention:** Adopt a standard naming convention, such as GRP_Sales_Read.

7. Security

7.1. Authentication

- **Multi-Factor Authentication (MFA):** Implement MFA for all privileged accounts and remote access.
- **Kerberos and NTLM:** Prefer Kerberos over NTLM for authentication due to its enhanced security features.

7.2. Authorization

- **Least Privilege Principle:** Assign permissions based on the principle of least privilege.
- **Role-Based Access Control (RBAC):** Use RBAC to streamline permission management.

7.3. Auditing and Monitoring

- **Audit Policies:** Enable auditing for key AD events, including logon attempts, account changes, and access to sensitive resources.
- **Monitoring Tools:** Utilize tools such as Microsoft Advanced Threat Analytics (ATA) to monitor AD for suspicious activities.

7.4. Security Baselines

- **Group Policy:** Use Group Policy Objects (GPOs) to enforce security baselines across the AD environment.
- **Hardening:** Follow best practices for hardening AD servers, including disabling unnecessary services and applying security patches.

8. Backup and Recovery

8.1. Backup Policies

- **Frequency:** Perform regular backups of AD, including system state and critical data.
- **Retention:** Retain backups for a minimum of 30 days, with longer retention for monthly and yearly backups.
- **Encryption:** Encrypt backups to protect data confidentiality.

8.2. Recovery Procedures

- **Disaster Recovery Plan:** Maintain a comprehensive disaster recovery plan, including procedures for restoring AD in the event of a failure.
- **Testing:** Regularly test backup and recovery processes to ensure reliability.

9. Change Management

9.1. Change Control

- **Approval Process:** All changes to the AD environment must be approved by the AD governance team.
- **Documentation:** Maintain detailed documentation for all changes, including the rationale, impact analysis, and rollback procedures.

9.2. Testing and Validation

- **Testing Environment:** Use a separate testing environment to validate changes before deploying them to production.
- **Post-Change Review:** Conduct post-change reviews to assess the impact and address any issues.

10. Incident Response

10.1. Incident Management

- **Detection:** Use monitoring tools to detect AD-related incidents promptly.
- **Response:** Follow a predefined incident response plan to mitigate and resolve incidents.
- **Reporting:** Report significant incidents to the AD governance team and senior management.

10.2. Root Cause Analysis

- **Investigation:** Perform root cause analysis for all major incidents to identify underlying issues.
- **Remediation:** Implement corrective actions to prevent recurrence.

11. Compliance and Auditing

11.1. Regulatory Compliance

- **Standards:** Ensure AD management complies with relevant industry standards and regulatory requirements, such as GDPR and ISO/IEC 27001.
- **Policies:** Regularly review and update policies to reflect changes in regulations.

11.2. Auditing

- **Internal Audits:** Conduct regular internal audits to assess compliance with AD policies and standards.
- **External Audits:** Facilitate external audits as required by regulatory bodies or business partners.

12. Training and Awareness

12.1. Training Programs

- **Administrator Training:** Provide comprehensive training for AD administrators, covering best practices, security, and management tools.
- **User Awareness:** Educate users on AD-related security policies, such as password management and phishing awareness.

12.2. Continuous Improvement

- **Feedback Loop:** Establish a feedback loop to capture lessons learned and improve training programs.
- **Updates:** Regularly update training materials to reflect new technologies and threats.

13. Documentation

13.1. Documentation Standards

- **Consistency:** Maintain consistent and up-to-date documentation for all aspects of AD management.
- **Accessibility:** Ensure documentation is easily accessible to authorized personnel.

13.2. Key Documents

- **Design Documents:** Include detailed AD design and architecture documents.
- **Operational Procedures:** Document all operational procedures, including user management, group management, and backup processes.
- **Security Policies:** Maintain comprehensive security policies for AD.

14. Roles and Responsibilities

14.1. AD Governance Team

- **Oversight:** Provide oversight and governance for all AD-related activities.
- **Approval:** Approve significant changes and policies related to AD.

14.2. AD Administrators

- **Management:** Manage day-to-day operations of the AD environment.
- **Implementation:** Implement changes and policies as approved by the governance team.
- **Monitoring:** Monitor AD for performance and security issues.

14.3. Security Officers

- **Security Oversight:** Ensure AD security policies are enforced and adhered to.
- **Incident Response:** Lead the response to AD-related security incidents.

14.4. Users

- **Compliance:** Comply with AD policies and procedures.
- **Reporting:** Report any issues or incidents related to AD.

15. Conclusion

Effective Active Directory management is essential for the security and efficiency of ISA Inc.'s IT infrastructure. By adhering to these policies and standards, we can ensure that our AD environment is robust, secure, and capable of supporting our business needs.

This document should be reviewed regularly and updated as necessary to address new challenges and changes in the IT landscape. By maintaining a well-managed AD environment, ISA Inc. can enhance security, improve efficiency, and support the organization's overall objectives.