NORTH Dakota | Information Technology

Be Legendary.™

Administrative Privilege Service Level Agreement

July 2024

In conjunction with NDIT's Enterprise Service Level Agreement, it acts as a Service Level Agreement between NDIT and customers

Contents

NDIT Administrative Privilege Service Level Agreement (SLA)

Introduction

The North Dakota Information Technology Department (NDIT) provides administrative privilege access following the principles of separation of duties and least privilege. This agreement outlines the terms and conditions for granting and managing administrative privileges to ensure secure and efficient operations.

Key Principles

Separation of Duties

Separation of Duties (SoD) is a critical security principle that reduces the risk of error, deficiency, inaccuracy, irregularity, and corruption among personnel. By dividing responsibilities among different individuals, NDIT ensures no single person has control over all aspects of any critical function.

Least Privilege

Least Privilege (LP) ensures users are granted only the minimum level of access necessary to perform their job functions. This principle limits access to sensitive data and systems, thereby reducing the risk of unauthorized access or potential security breaches.

Administrative Access Review

NDIT is currently reviewing administrative access on an agency-by-agency basis. The objectives are to:

- Remove unnecessary privileged access.
- Reevaluate necessary access for fit into two categories: Endpoint Privilege Management (EPM) or a Privileged (PRV) account.

Categories of Access

Endpoint Privilege Management (EPM)

EPM is the default choice for administrative access. It provides the necessary access at a cost of $3.50 per user/month.

Privileged (PRV) Account

PRV accounts require approval from the NDIT security division's Governance, Risk, and Compliance (GRC) department and require MFA to be enabled. Agency Director or Delegate must sign a risk acceptance waiver for each person/account, with an annual reevaluation and signature requirement.

Note: PRV accounts must be used at least once every 60 days, or they will be automatically disabled. The password must also be reset every 60 days.

Request Process

Agencies can request an EPM license by submitting a request to desktop services, or a PRV account evaluation by submitting a generic request to security, through the ServiceNow portal.

Terms and Conditions

1. **Eligibility**: Only users who require administrative access to perform their job duties are eligible.
2. **Approval Process**:
    - EPM access requests will be reviewed and approved based on job requirements.
    - PRV account requests will be reviewed and approved based on job requirements and require approval from the GRC department and the signing of a risk acceptance waiver.
3. **Annual Review**: All PRV accounts must undergo an annual review, requiring reevaluation and signing of the risk acceptance waiver.
4. **Cost**:
    - EPM: $3.50 per user/month.
    - PRV: $7.10 per user/month through June 2024, $7.85 per user/month starting July 2025.
5. **Compliance**: Users granted administrative privileges must comply with NDIT's security policies and procedures.
6. **Audit and Monitoring**: NDIT reserves the right to audit and monitor the use of administrative privileges to ensure compliance with security policies.
7. **Revocation of Access**: NDIT may revoke administrative privileges at any time if a user is found to be in violation of security policies or if their job duties no longer require such access.

Responsibilities

NDIT

- Review and process access requests in a timely manner.
- Conduct regular audits and reviews of administrative access.
- Provide necessary training and support for users with administrative privileges.

Agencies

- Submit accurate and justified access requests through the ServiceNow portal.

- Ensure users with administrative privileges understand and adhere to security policies.
- Participate in the annual review process for PRV accounts.

Users

- Use administrative privileges responsibly and only for intended job functions.
- Report any security incidents or breaches immediately to NDIT.
- Complete any required training related to administrative access and security policies.

Conclusion

This SLA establishes the framework for managing administrative privileges within NDIT, ensuring adherence to security principles, and maintaining the integrity of IT systems. By following this agreement, NDIT aims to provide secure, efficient, and controlled access to necessary resources, supporting the overall mission of the organization.

Modifications

Date	SLA Modifications