

Managed Identity Protection

Minnesota IT Services (MNIT) offers Managed Identity Protection (IDP) to local government entities to protect their users' digital identities and accounts from unauthorized access.

In partnership with MNIT's managed detection and response (MDR) vendor, managed IDP service delivers continuous, around-the-clock monitoring of identity activity across on-premises and cloud environments. Managed IDP provides real-time detection of suspicious behavior and rapid, expert-led response to stop threats before they escalate into costly incidents.

Key benefits of Managed IDP

- Stronger protection against account takeover, ransomware, and fraud.
- Real-time visibility into identity risk and suspicious activity.
- Immediate response actions, including MFA enforcement and credential remediation.
- Actionable guidance and continuous optimization from vendor experts.
- 24/7 monitoring and threat hunting, reducing the burden on internal IT and security teams.

How Managed IDP works

Managed IDP combines advanced identity monitoring technology and 24/7 MDR service to:

- Identify, investigate, and remediate suspicious account activity in near real time.
- Prevent lateral movement after an account has been compromised.

Managed IDP uses behavioral analytics, risk-based access controls, and expert-led response, to help stop a cyberattack. Detecting and mitigating threats early can reduce the risk of ransomware and account compromise and maintain the availability of critical public services.

Local government entities can use Managed IDP to:

- Prevent credential compromise/phishing attacks.
- Detect abnormal login behavior.
- Force multi-factor authentication (MFA) or to block access.
- Reset compromised credentials.
- Detect lateral movement in Active Directory.
- Identify suspicious authentication patterns.
- Stop privilege escalation.
- Contain spread across systems.
- Prevent privileged account misuse.
- Enforce strong authentication policies.
- Detect unusual administration behavior.
- Prevent unauthorized access to critical systems.
- Ensure hybrid/cloud identity protection.
- Protect on-premises, hybrid, and security-as-a-service identity environments.

Decide if Managed IDP can help your organization

Managed IDP is ideal for local government entities that:

- Employ limited cybersecurity staff or have no 24/7 security operations center.
- Seek to add or enhance existing security/identity protection capabilities.
- Rely on Active Directory or Entra ID.
- See increased risks for phishing or credential compromise.
- Must meet compliance requirements (Criminal Justice Information Services, regulatory frameworks.)

Eligibility and cost

Managed IDP is available to local government entities, including counties, cities, townships, K-12 school districts, public-sector critical infrastructure, and Tribal Nations that also use MNIT's Managed Detection and Response service.

The cost is $8 per user, per year. Entities must enroll every user in their domain. Entities will be billed monthly at a rate of $0.6667/per user, per month.

Get started

Contact MNIT's Cyber Navigator team for information or get signed up:
CN.MNIT@state.mn.us