

# Security Services

Service Description Version 1.00

---

Effective Date: 07/01/2012

---

## Purpose

This Enterprise Service Description is applicable to **Security Services** offered by the MN.IT Services and described in the MN.IT Services Catalog. This document describes the services and features that are included with the **Security Services** offering.

## Overview

This Service Description includes three distinct Security Services offerings: Access Control to Systems, Security Incident Response and Forensics, and Security Awareness and Training. The sections below provide a description of these services; for additional details, see the applicable "Security Services Service Level Agreement" document.

## Access Control to Systems

The purpose Access Control to Systems is to create, maintain, and provision identities that may need some level of trusted access to State assets and to manage their associated attributes. Access Control to Systems is requested through the MN.IT Services Service Desk. Creation of identities is typically performed during the onboarding process.

Key service tasks include:

- Establish Identities
- Manage Identities
- Manage encryption keys and security certificates to provide trust for transactions and web sites

Currently, the State of Minnesota manages identities via stand-alone, disparate systems and varied levels of data protection. This approach has led to redundant operations, less than adequate security controls, with wide variances in adherence to and interpretations of security standards, and installations of varied software solutions.

A centralized Identity and Access Management (IAM) Service is being refreshed and we are in the process of migrating the first applications. This initiative aims at implementing an enterprise IAM Service to address these issues.

Access Control to Systems is a broad administrative and technology area that deals with identifying individuals in a system (such as a network or an application) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. Access management is the enabling service that ensures access is granted to assets, such as information, technology, and facilities must be made available (accessible) for use. This requires that persons (employees and citizens), objects (such as systems), and entities (such as business partners) have sufficient (but not excessive) levels of access to these assets.

The challenge of authenticating and managing increased user accounts with the appropriate level of access requires an integrated security framework that addresses aspects of user and role administration, authentication, authorization, and auditing/reporting at an enterprise level. The conceptual overview below illustrates how the IAM framework provides various services to citizens, employees and business partners.

**Figure 1: Identify and Access Management Framework**

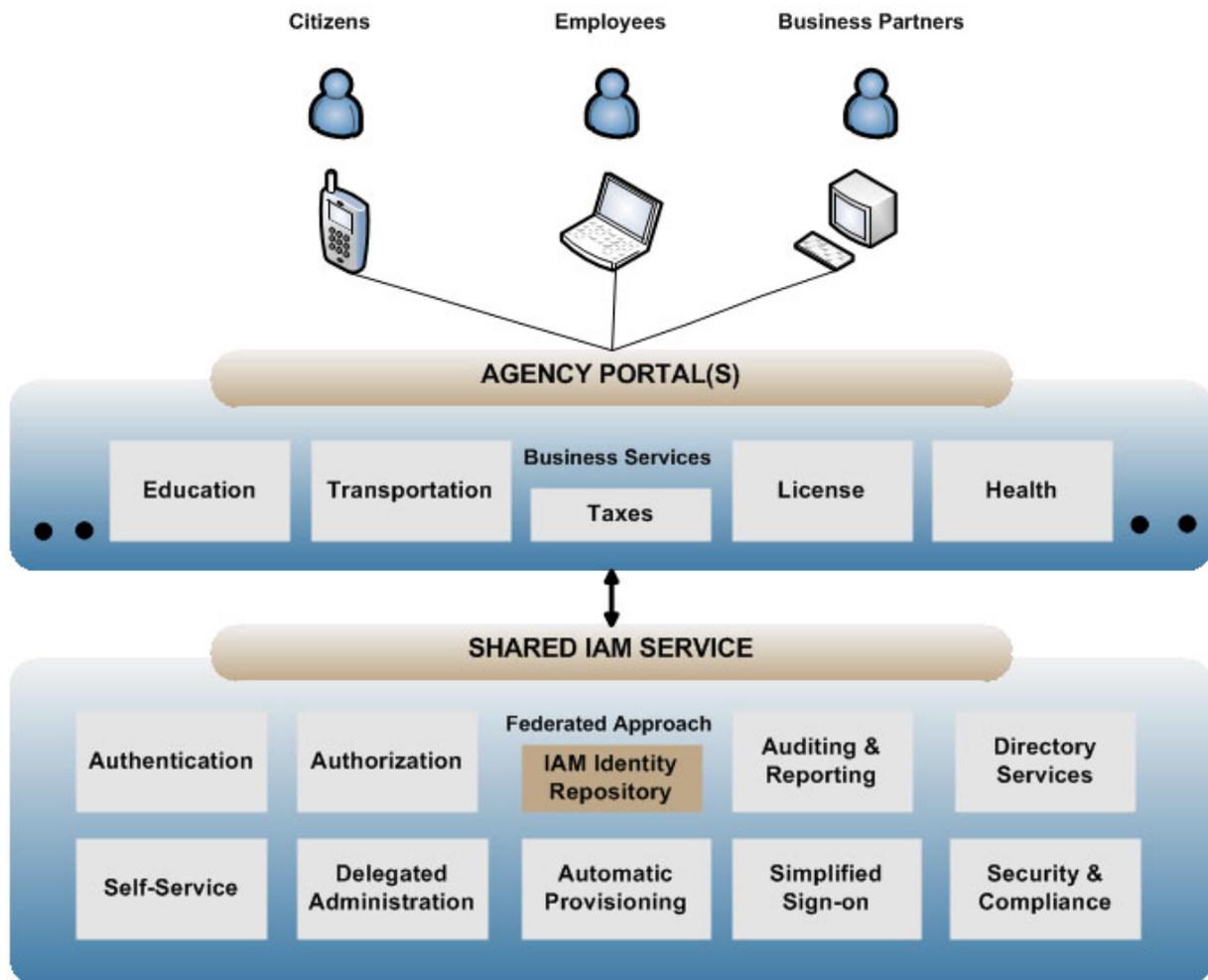


Figure 1 illustrates the following framework:

- There are three high-level types of users: Citizens, Employees, and Business Partners.

- Through laptops, desktops, or mobile devices; these users access business services such as Education, Transportation, Taxes, License, Health, etc. through various agencies portals.
- The Shared IAM Service supports the Business Services with: Authentication, Authorization, Federated Approach to IAM Identity Repository, Auditing & Reporting, Directory Services, Self-Service, Delegated Administration, Automatic Provisioning, Simplified Sign-on, and Security & Compliance.

## Security Incident Response and Forensics

Security Incident Response and Forensics are professional services that utilize multiple tools to resolve the business issues below. Security Incident Management is a process to stop unwanted activity, limit damage, and prevent recurrence of security events. Computer forensics is a standardized process to determine the cause, scope, and impact of incidents and limit damage that may be used in legal or human resource actions.

### Report an Incident

Security Incident Response and Forensics is requested through the MN.IT Services Service Desk.

### Security Incident Management Objectives

The service objectives address some specific aspects of the process where the timeliness of a response is critical to the successful management of an incident. Respect to confidentiality and sensitivity of the investigations, limiting access to information to a need-to-know basis is paramount to this service. The bulk of the service is approached in a project fashion with designated milestones, where an estimated level of effort (LOE) is provided in labor-hours.

### Computer and Data Forensics Objectives

Computer and Data Forensics service is approached as a project with designated milestones, where a LOE is provided in labor-hours when the request is accepted and then refined when the plan is developed. This service can be dependent on resources outside the span of control of the service team; these dependencies are identified in the plan, and can affect the ability to meet the service objectives.

## Security Training and Awareness

Security Training and Awareness provides employees at all levels with relevant security information and training to lessen the number of security incidents. Security Training and Awareness services are requested through the MN.IT Services Service desk. MN.IT Services can provide training and support in the following areas:

- Generalized Security and Awareness
- Customized Security Awareness and Training for unique requirements
- Online training from the SANS Institute (SysAdmin, Audit, Networking, and Security) "Securing the Human"

## Benefits

### Access Control to Systems

- **Simplifies User Experience** - provides a better experience for users of state services by providing access through fewer user IDs and passwords.
- **Reduces Costs** - leverages a centralized identity management solution when customers develop/refresh their government systems. Typically, customers have multiple applications that require Access Control to

Systems. The service eliminates the need for each customer to manage users for each system. This can be done centrally and done once. In addition, service desk costs can be lowered through self-service account management.

- **Improves Security** – removes inactive accounts that no longer have a valid owner across all platforms and applications with a single action.
- **Simplified Integration** – integrate government services and external entities such as business partners.

### **Security Incident Response and Forensics**

Security Incident Response and Forensics customers receive these benefits:

- Security professionals will:
  - Manage security incident case assignments and the security investigation process with a need-to-know basis
  - Mobilize emergency and third party investigation and response processes, when necessary
  - Consult with system owners to help quarantine incidents and limit damage
  - Consult with HR on violations of appropriate use policy
  - Communicate with law enforcement, when necessary
- Business issues addressed:
  - Customer Specific Incidents
  - Denial of Service
  - Security Policy Violations
  - Malware
  - Physical Loss/Theft/Damage
  - Unauthorized Access
  - Unauthorized Alteration/Destruction
  - Unauthorized Disclosure

### **Security Awareness and Training**

Security Awareness and Training customers receive these benefits:

- Compliance with security awareness and training policies
- Security professionals will:
  - Coordinate general security awareness training for all employees and contractors
  - Coordinate security training for groups with specialized needs, such as application developers
  - Provide persistent and regular messaging relating to cyber security threats and vulnerabilities

### **Standard Features**

This section describes the standard features of Security Services. Where applicable, customer options are noted, along with feature limits and the responsibilities of MN.IT Services.

## Access Control to Systems

- **Statewide ID** provides a better experience for users of state services by providing access through a single user ID and password. It is much easier for the state and the user to have a single ID to manage the authorization than have multiple user IDs.
- **Identity Proofing** provides a level of trust for user identities accessing your applications. Using a central identity repository eliminates the need for each customer to perform identity proofing.
- **Single Administration Point** eliminates the need for each customer to manage identities in multiple places. Inactive accounts can be removed from all platforms and applications with a single action. This can be done centrally and done once.
- **Privileged Account** management is provided with specialized tools and processes. This ensures system changes can be made whenever necessary without concern for undetected misuse of resources.
- **Account Management** is provided through the MN.IT Services Service Desk. Service Desk staff ensures password resets are completed per business requirements.
- **Security Certificates** can be managed by MN.IT Services so systems are secure and the certificates are not expired.

## Access Control to Systems Customer Responsibilities

1. Integration and migration technical support is part of the basic service, but the application integration with the IAM Service is the responsibility of the application owner.
2. The customer is responsible for assisting in the operation of the Access Control to Systems Service. These responsibilities are:
  - a. Maintain the list of delegated administrators.
  - b. Maintain list of citizen, employee, and business partner identities.
  - c. Provide MN.IT Services with logging and reporting requirements based on regulatory compliance.
  - d. Support disaster recovery testing and declarations.
  - e. Maintain contact list to respond to security incidents.

## Security Incident Response and Forensics

Security Incident Response and Forensics is responsible for determining the cause, scope, and impact of incidents to stop unwanted activity, limit damage, and prevent recurrence. Computer and Data Forensics is a standardized process that determines the cause, scope, and impact of incidents that may be used in legal or human resource actions.

### Security Incident Management Process

Security Incident Management is a process that is triggered by the detection of an event. When an event is detected this process evaluates the event to determine if a security incident has occurred. The Security Incident Management consists of five processes described on the next page:

**Figure 2: Security Incident Management Process Flow**



Figure 2 illustrates the following process flow:

- **Incident Recording** includes the contact information and required data to be collected at the time of recording
- **Incident Validation** includes the processes and tools for validating recorded security events
- **Incident Classification** includes the definitions and classifications of validated security incidents
- **Incident Investigation** includes steps and procedures for isolating, eradicating and remediating security incidents
- **Incident Reporting** includes the required processes for reporting on security incidents

The service objectives address some specific aspects of the process where the timeliness of a response is critical to the successful management of an incident. The bulk of the service however is approached in a project fashion with designated milestones, where an estimated LOE is provided in labor-hours.

Computer and Data Forensics Process

Computer and Data Forensics can be a part of Security Incident Management, but is also offered as a stand-alone service to support customer-specific incident management, or to provide additional, in-depth collection and analysis of data objects. The computer and data forensics service consists of four processes.

**Figure 3: Computer and Data Forensics Process Flow**

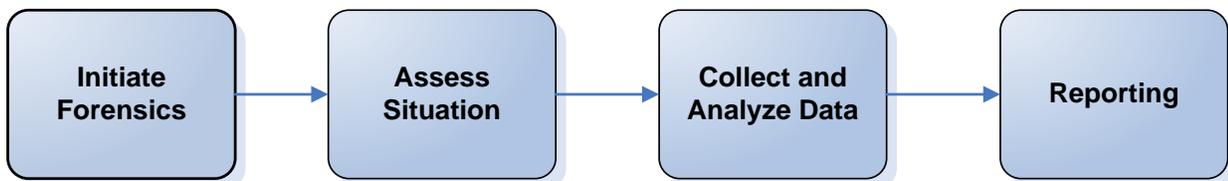


Figure 3 illustrates the following process flow:

- **Initiate Forensics** includes the contact information and required data to be collected at time of recording
- **Assess Situation** includes insuring the information is complete, establishing the legal authority, and developing the scope and the plan.
- **Collect and Analyze Data** includes gathering and analyzing all of the pertinent data.
- **Reporting** includes the creation and issuance of the final report

**Security Incident Response and Forensics Customer Responsibilities**

The success of incident management is predicated on the timeliness of the identification and notification of a security event. It is the customer’s responsibility to contact the MN.IT Services Service Desk promptly to initiate the security incident management process.

**Security Awareness and Training**

Security Awareness and Training is responsible for providing employees at all levels with relevant security information and training to lessen the number of security incidents.

**Security Awareness and Training Service Features are:**

- Security Awareness and Training content developed and made available
- Coordinate and provide training for:
  - All employees and contractors
  - Groups with specialized needs, such as application developers
  - Special events such as: National Cyber Security Awareness Month
- Provide persistent and regular messaging relating to cyber security threats and vulnerabilities

### **Security Awareness and Training Customer Responsibilities**

When the customer has a training requirement, the customer has the responsibility to contact MN.IT Services.

### **Related Information**

- Minnesota Statutes 2011 Chapter 16E ([Office of Enterprise Technology](#))
- Minnesota Statutes 2011 Chapter 13, Minnesota Data Practices Act
- Enterprise Technology Fund 970 Rate Schedule
- Enterprise Information Security Policies and Standards on MN.IT website
- Operational documents / information on MN.IT website
- Security Services Service Level Agreement
- Identification and Authentication Security Standard
- Identity and Access Management Architecture Standards
- Information Security Incident Management Standard
- Information Security Incident Management Policy
- Information Security Incident Management Process Overview
- Computer and Data Forensics Process Overview
- Section 7 – Information Security