Security Incident Response
Service Level Agreement (SLA)
By
Information Technologies (UNM IT)
For
UNM Data Owners (Customer)

Effective Date:	
Document Owner:	Jeff Gassaway

Related/Referenced Documents:

Table of Contents

1 General Overview

This is an SLA between the Customer, UNM Data Owners, and UNM IT to document the provision of:

- The Information Security Incident Response services;
- The responsibilities of UNM IT as a provider of these services;
- The responsibilities of the End-Users and Customers receiving these services;
- The financial arrangements associated with the services.

This SLA shall be effective as of the Effective Date set forth on the cover page and will continue until revised or terminated.

2 Service Description

UNM IT documents services and associated fees in the UNM IT service catalog, http://it.unm.edu/servicecatalog.

2.1 Service Scope

UNM IT assists units in which security events, incidents, and/ or breaches occur. This work is performed on behalf of UNM Data Owners, as required for contractual, policy, and regulatory compliance. Such responses can include reviewing, recovering, collecting, and preparing digital evidence in support of authorized investigations, and may include additional compliance activities, depending upon the kind and scale of event or incident.

2.1.1 End-User Requirements to Use the Service

- Report any suspected or actual information security events, incidents, and/ or breaches to 888-899-6092 and/or email security@unm.edu with contact information (do not put sensitive information about a security incident in email);
- Comply with directions from UNM Information Security professionals and with UNM authorized investigative bodies. Ensure unit resources are available to assist in the incident response.

2.1.2 Boundaries of Service Features and Functions

- UNM units are responsible for the costs of incident response for incidents that occur in their areas;
- Authorized investigative bodies are responsible for determining non-IT root causes of information security incidents and of non-information security and privacy response;
- UNM IT, in consultation with other UNM investigative bodies, will evaluate compliance with the following regulatory, contractual, or policy requirements:
    - Family Education Rights and Privacy Act (FERPA);
    - Health Insurance Portability and Accountability Act (HIPAA);
    - Gramm Leach Bliley Act, Aka Financial Services Modernization Act (GLBA);
    - Payment Card Industry (PCI);
    - Other regulatory or contractual areas will be provided, as needed, by authorized third party subject matter experts and service providers, for an additional fee;
- UNM IT may utilize third-party contracted resources to evaluate and/ or assist in the response of reported events or incidents, depending upon available capacity.

2.2 Service Level Performance

2.2.1 General Service Levels

- Information Security staff will respond to entities that report incidents or suspected incidents within 60 minutes of being notified of such information security incidents;

- Information Security will facilitate the development and execution of the incident response utilizing UNM's Incident Response Plan (IRP) template.

2.2.2 Specific Service Levels

This section intentionally left blank.

3 Roles and Responsibilities

3.1 UNM IT Responsibilities in Support of the Service

UNM IT responsibilities and/or requirements in support of this SLA include:

- Facilitating defining the scope of the Incident Response Plan (IRP);
- Facilitating the implementation, discovery, and execution of the IRP;
- Supplying subject matter expertise regarding information security and privacy to specific incidents;
- Providing access to information security resources and services to units to support the response, which may include:
    - Penetration testing;
    - Vulnerability scanning;
    - Computer forensics imaging and analysis;
    - Log review and analysis;
    - Regulatory and contractual compliance requirements;
- Coordinating with vendors to support incident response;
- Negotiating and managing any third-party services;
- Qualifying incidents may have institutional risk management funds available to address the response to some kinds of incidents. UNM IT will assist in facilitating these discussions where applicable;
- In addition, UNM IT will provide UNM Data Owners with standard information security incident response overview including:
    - Template engagement document;
    - Template incident response overview with
        - Roles and responsibilities;
        - Rates for hours/ services;
        - IRP template;
- Prepare and deliver to the appropriate UNM Data Owner and Investigative Authority, confidential:
    - Updates and briefings as details become available, as appropriate;
    - Final report with recommendations to mitigate and/ or prevent incident recurrence;
- Friendly, courteous and efficient service;
- Continuous effort to develop and improve services.

3.2 Customer Responsibilities in Support of the Service

Customer, for the purposes of this SLA, are UNM's Data Owners that are responsible for Personally Identifiable/Sensitive and Protected Information (PII/ SPI) in their areas.

Customer responsibilities and/or requirements in support of this SLA include:

- Technical and Business point of contact for each impacted unit to assist in the development of the IRP;
- Timely and complete access to systems, staff, logs, and communications related to the incident and/ or the incident causes;
- Appropriate business and technical staff for the duration of the information security incident;
- IT Strategic Advisory Committee to collaborate with UNM IT on the service framework to satisfy the University of New Mexico business requirements;

- Comply with UNM Business Policies 2500, 2520, 2580 and 7215:
  https://policy.unm.edu/university-policies/2000/2500.html
  https://policy.unm.edu/university-policies/2000/2520.html
  https://policy.unm.edu/university-policies/2000/2580.html
  https://policy.unm.edu/university-policies/7000/7215.html

4 Hours of Coverage and Escalation

4.1 Hours of Coverage

Security Incident Response is conducted as articulated in the IRP.

4.2 Service Exceptions to Coverage

This section intentionally left blank.

4.3 Escalation and Exceptions

If you are not satisfied with the performance of the service or incident/request process, please contact the Service Owner or Service Manager.

UNM IT Contact	
Service Owner	Jeff Gassaway base@unm.edu Information Security & Privacy Officer
Service Manager	TJ Martinez tjm@unm.edu Director of IT Customer Services

To request exceptions to defined service levels based on exceptional business needs, please email cio@unm.edu. The Office of the CIO / UNM IT will respond to the message within 5 business days and escalate any mutually agreed upon exceptions to the IT Strategic Advisory Council (ITSAC) and UNM's Senior Administration for review, approval, and funding, if necessary.

5 Service Requests

This section intentionally left blank.

6 Incidents

This section intentionally left blank.

7 Maintenance and Service Changes

This section intentionally left blank.

8 Pricing and Billing

The Information Security services hourly rate is UNM IT documents services and associated fees in the UNM IT service catalog, http://it.unm.edu/servicecatalog.

Charges for UNM IT services are billed monthly in arrears and post automatically to UNM unit indices on the 1st business day of each month. Monthly bill detail for UNM IT charges can be accessed using the UNM IT Billing Portal at http://it.unm.edu.

9 Reviewing and Reporting

9.1 System Performance and Availability Reporting

This section intentionally left blank.

9.2 SLA Reviews

UNM IT is responsible for facilitating reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties.

This SLA contains the complete agreement between the parties and shall not be changed, amended or altered except in writing and signed by each party.

10 Approvals

UNM IT: University of New Mexico CIO	**CUSTOMER:**
By: Gilbert Gonzales	By: _____
Title: Chief Information Officer	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____