****

Memorandum of Agreement

**Between**

**New Mexico Institute of Mining and Technology**

**And**

**“Provider”**

This Memorandum of Agreement (MOA) is made effective between New Mexico Institute of Mining and Technology (“NMIMT” or “Institution”) whose place of business is at 801 Leroy Place, Socorro, NM 87801, and between “Provider”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ whose place of business is at\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

# CONFIDENTIAL INFORMATION

Provider including its employees and subcontractors, to this contract may have or gain access to confidential data or information owned or maintained by the other Provider in the course of carrying out its responsibilities under this contract.  Provider shall presume all information received from the State or to which it gains access pursuant to this contract is confidential.  Provider information, unless clearly marked as confidential and exempt from disclosure under the Inspection of Public Records Act, NMSA 14-2, shall be considered public.  No confidential data collected, maintained, or used in the course of performance of the contract shall be disseminated except as authorized by law and with the written consent of the disclosing Provider, either during the period of the contract or thereafter.  The receiving Provider must return any and all data collected, maintained, created or used in the course of the performance of the contract, in whatever form it is maintained, promptly at the end of the contract, or earlier at the request of the disclosing Provider, or notify the disclosing Provider in writing of its destruction.  The foregoing obligations shall not apply to confidential data or information lawfully in the receiving party’s possession prior to its acquisition from the disclosing party; received in good faith from a third Provider not subject to any confidentiality obligation to the disclosing Provider; now is or later becomes publicly known through no breach of confidentiality obligation by the receiving Provider; or is independently developed by the receiving party without the use or benefit of the disclosing Institution’s confidential information.

# NO WAIVER OF RIGHTS

Except as specifically waived in writing, failure by either party to exercise or enforce a right does not waive that party’s right to exercise or enforce that or other rights in the future.

# AUDIT/RETENTION OF RECORDS

Provider and its subcontractors shall maintain books and records relating to the performance of the contract or subcontract and necessary to support amounts charged to the State pursuant the contract or subcontract.  Books and records, including information stored in databases or other computer systems, shall be maintained by the Provider for a period of three (3) years from the later of the date of final payment under the contract or completion of the contract, and by the subcontractor for a period of three (3) years from the later of final payment under the term or completion of the subcontract.  If Federal funds are used to pay contract costs, the Provider and its subcontractors must retain their respective records for five (5) years.  Books and records required to be maintained under this section shall be available for review or audit by representatives of:  the procuring Agency, the Auditor General, the Executive Inspector General, the Chief Procurement Officer, State of New Mexico internal auditors or other governmental entities with monitoring authority, upon reasonable notice and during normal business hours.  Provider and its subcontractors shall cooperate fully with any such audit and with any investigation conducted by any of these entities.  Failure to maintain books and records required by this section shall establish a presumption in favor of the State for the recovery of any funds paid by the State under this contract or any subcontract for which adequate books and records are not available to support the purported disbursement. The Provider or subcontractors shall not impose a charge for audit or examination of the Provider’s or subcontractor’s books and records.

#  INDEMNIFICATION AND LIABILITY

Provider shall indemnify and hold harmless Institution, its agencies, officers, employees, students, agents and volunteers from any and all costs, demands, expenses, losses, claims, damages, liabilities, settlements and judgments, including in-house and contracted attorneys’ fees and expenses, arising out of: (a) any breach or violation by Provider of any of its certifications, representations, warranties, covenants or agreements; (b) any actual or alleged death or injury to any person, damage to any real or personal property, or any other damage or loss claimed to result in whole or in part from Provider’s negligent performance; (c) any act, activity or omission of Provider or any of its employees, representatives, subcontractors or agents; or (d) any actual or alleged claim that the services or goods provided under this contract infringe, misappropriate, or otherwise violate any intellectual property (patent, copyright, trade secret, or trademark) rights of a third party.  In accordance with Article IX, §8 of the Constitution of the State of New Mexico and *State Office Bldg Comm’n v. Trujillo,* 1941-NMSC-051, 46 N.M. 29, agencies of the State may not indemnify private parties absent express statutory authority permitting the indemnification.

# INSURANCE

Provider shall, at all times during the term and any renewals maintain and provide a Certificate of Insurance naming the State as additionally insured for all required bonds and insurance.  Certificates may not be modified or canceled until at least thirty (30) days’ notice has been provided to the State.  Provider shall provide: (a) General Commercial Liability occurrence form in amount of $1,000,000 per occurrence (Combined Single Limit Bodily Injury and Property Damage) and $2,000,000 Annual Aggregate; (b) Auto Liability, including Hired Auto and Non-owned Auto, (Combined Single Limit Bodily Injury and Property Damage) in amount of $1,000,000 per occurrence; and (c) Worker’s Compensation Insurance in amount required by law.  Insurance shall not limit Provider’s obligation to indemnify, defend, or settle any claims.

# INDEPENDENT CONTRACTOR

Provider shall act as an independent contractor and not an agent or employee of, or joint venture with the State or other external entity not included in this MOA.  All payments by the Institution shall be made on that basis.

# SECURITY REQUIREMENTS

The New Mexico Institute of Mining and Technology (NMT) has specific security requirements for information and systems.  Provider must ensure these requirements are fully understood and allocate sufficient project time and resources to address the security requirements.

An information security risk assessment, data classification and system categorization process and the submission of a system security plan must be completed and submitted to the NMT Information Security Officer, Information Security Division of Information Technology and Communication (ITC) prior to the commencement of system development or solution delivery activities. Provider must participate with the risk assessment and data classification and system categorization process. The formal risk assessment, data classification and system categorization process will be administered by the Information Security Team, Division of Information Technology and Communication (ITC).  Vender program and project management personnel must ensure the coordination of these activities with NMT program and project management personnel. If not specifically addressed in other Provider Information Technology Requirements, Provider must adhere to State of New Mexico and NMT security policies, procedures, and standards.

Provider must also adhere to a minimum security baseline as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Systems and Organizations. If not specifically addressed in other Provider Information Technology Requirements, Providers must assure the adoption of, at minimum, the low security control baselines.  Exceptions to this requirement must be approved by the NMT Information Security Officer, Information Security Division of Information Technology and Communication (ITC).

Cloud solutions must adhere to recommendations of the Cloud Security Alliance. Providers may find guidance and cross-referencing to the NIST 800-53, Revision 4 with the Cloud Security Alliance controls at:

 https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

State and Federal laws, rules and regulations as well as industry-specific guidelines require specific and often enhanced security controls on information and systems.  The State of New Mexico is required to comply with the below laws, standards and regulations.  Providers must ensure compliance with the below as appropriate based upon the formal risk assessment to include a data classification and system categorization process.

# SYSTEM SECURITY CONSIDERATIONS

*The following items must be included and answered in the Agreement.*

## General Information/Data Description.

*[At a general level, describe the information/data being made available, exchanged, or passed one way only, by the interconnection of the two systems.]*

## Services Offered.

*[Describe the nature of the information services (e.g. E-mail, FTP, database query, file query, general computational services, etc.) offered over the interconnected system by each participating organization.]*

## Data Sensitivity.

1. Parties are required to configure systems to mark metadata in environments where Data Loss Prevention (DLP) and Network Access Control (NAC) technology is being used.
2. Parties must:

### In accordance with all applicable statutory, regulatory and contractual compliance obligations, implement and govern controls to protect NMT data wherever it is stored, transmitted and processed;

### Define retention periods for both sensitive and non-sensitive data;

### Dispose of, destroy, erase, and / or anonymizes data once it is no longer necessary for business purposes;

### Maintain strict control over the storage and accessibility of media;

### Maintain inventories of sensitive data under their control.

1. State and Federal laws, rules and regulations as well as industry-specific guidelines require specific and often enhanced security controls on information and systems. The State of New Mexico is required to comply with the below laws, standards and regulations. Providers must ensure compliance with the below as appropriate based upon the formal risk assessment to include a data classification and system categorization process.

|  |  |  |
| --- | --- | --- |
| T-1 | **External Authority** | **Information Requirements** |
| FERPA | Family Educational Rights and Privacy | https://studentprivacy.ed.gov/node/548/ |
| GLBA | Gramm-Leach-Bliley Act | https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 / Public Law 104-191 | https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996 |
| HITECH | Health Information Technology for Economic and Clinical Health / Section 13410(d) | https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html |
| PCI | PCI Data Security Standard | https://www.pcisecuritystandards.org/document\_library/?category=pcidss&document=pci\_dss |
| New Mexico's Privacy Protection Act | §§ 57-12B-1 et seq. of Article 12B of Chapter 57 | https://nmonesource.com/nmos/nmsa/en/item/4423/index.do#!fragment/zoupio-\_Toc110332560/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgEYOAGAZl4BMAVgBs3AJQAaZNlKEIARUSFcAT2gByDZIiEwuBEpXqtOvQZABlPKQBC6gEoBRADJOAagEEAcgGEnkqRgAEbQpOzi4kA |
| § 14-6-1 of Article 6 of Chapter 14 of the N.M. Statutes | Health Data | https://nmonesource.com/nmos/nmsa/en/item/4383/index.do#!b/14-6-1 |
| Article 12 of Chapter 30 of the N.M. Statutes | Abuse of Privacy | https://nmonesource.com/nmos/nmsa/en/item/4371/index.do#!fragment/zoupio-\_Toc113359153/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgEYOBmbgVgCcHPtwCUAGmTZShCAEVEhXAE9oAcjXiIhMLgQKlqjVp16QAZTykAQqoBKAUQAyDgGoBBAHIBhB+NJgAEbQpOyiokA |

## Trusted Behavior Expectations.

1. Each system is expected to protect the information belonging to the Institution through the implementation of a security program that provides for defense against intrusion, tampering, virus, detection.
2. Covered entities are expected to apply a risk-based approach minimize its attack surface area through aggressive vulnerability management and patching operations.
3. Provider is expected to implement and govern processes and documentation to facilitate the implementation of a Continuity of Operations (COOP) policy, as well as associated standards, controls and procedures.

## Formal Security Policy.

1. Provider shall protect the confidentiality, integrity, availability and safety of the Institution data and systems, regardless of how its data is created, distributed or stored. Digital security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all statutory, regulatory and contractual obligations.
2. Provider privacy and security policies and standards shall be available upon request in a consolidated document, the Information Security Program (ISP) that shall be:

### Endorsed by executive management;

### Disseminated to the appropriate parties to ensure all NMT personnel understand their applicable requirements.

## Incident Reporting.

1. Provider is required to established processes and technical measures to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.
2. Provider is required to establish forensic procedures, including chain of custody, to preserve evidence to support potential legal action subject to the relevant jurisdiction after a cybersecurity incident.
3. For actual or suspected cybersecurity incidents:

### Provider is responsible for reporting system weaknesses, deficiencies, and vulnerabilities to the Institution as quickly as possible;

### Information security events should be reported to the Institution as quickly as possible;

1. If a breach occurs, breach notification procedures must occur without unreasonable delay, except:

### When a law enforcement agency has determined that notification will impede a criminal investigation; or

### In order to discover the complete scope of the breach and restore the integrity of the system.

## Audit Trail Responsibilities.

1. Provider is required to configure system to produce audit records that contain sufficient information to, at a minimum:

### Establish what type of event occurred;

### When (date and time) the event occurred;

### Where the event occurred;

### The source of the event;

### The outcome (success or failure) of the event;

### The identity of any user / subject associated with the event.

1. Provider is required to configure systems to record at least the following audit trail entries for all system components for each event:

### User identification;

### Type of event;

### Date and time;

### Success or failure indication;

### Origination of event;

### Identity or name of affected data, system component or resource.

1. Provider is required protect sensitive data contained in log files.
2. Provider is required to limit Personal Information (PI) contained in audit records to the elements identified.
3. Provider is required to protect and where required encrypt, log files that may contain sensitive data:

### Passwords in the clear;

### Social Security Numbers;

### Driver’s License Numbers;

### Protected Health Information;

### Insurance Policy Numbers;

### Credit Card Numbers;

### Student ID Numbers;

### Employee ID Numbers;

### Bank Account Numbers;

### Covered Defense Information (CDI) Categories.

## Security Parameters.

1. All Parties are required to protect NMT’s systems and data in accordance with applicable statutory, regulatory and contractual compliance obligations;
2. Provider shall establish procedures, supporting business processes and implement technical measures to ensure the continuity and availability of operations while operating in other-than-normal conditions;
3. Unless otherwise protected by NMT-defined alternative physical safeguards, Provider must:

### Implement cryptographic mechanisms to prevent unauthorized disclosure of information;

### Detect changes to information during transmission;

### Systems prevent unauthorized and unintended information transfer via shared system resources;

## Training and Awareness.

1. Provider is require to ensure all users are made aware of the security and privacy risks associated with their roles and that users understand the applicable statutory, regulatory and contractual compliance requirements related to the security and privacy of systems and data within their sphere of influence.

This Agreement constitutes the entire agreement and understanding of the Provider and the Institution with respect to the subject matter hereof, and is intended as the Provider’s final expression and complete and exclusive statement of the terms thereof, not to supersede all prior or contemporaneous agreements, representations, promises and understandings, whether written or oral. Neither Party is to be bound by any pre-printed terms appearing in the other Party’s form documents, tariffs, purchase orders, quotations, acknowledgments, invoices, or other instruments. This Agreement may be amended or modified only by an instrument in writing signed by both Parties.

This Agreement is valid for the entire term of our contractual relationship, unless otherwise documented, from the last date on either signature below.  At that time it will be reviewed, updated if necessary, and revalidated.  This agreement may be terminated upon 30 days advanced notice by either party or in the event of a security exception that would necessitate an immediate response.

New Mexico Institute of Mining & \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Technology Provider

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title Title

|  |  |
| --- | --- |
|  |  |
|  |  |