WHEREAS, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and its implementing regulations codified at 34 C.F.R 99. 1 et seq. make personally identifiable student information in education records confidential and, subject to certain exceptions, prohibits the disclosure of such information to third parties,

WHEREAS, FERPA and its implementing regulations allow for an educational agency or institution to share personally identifiable student-level data with contractors performing work on their behalf,

WHEREAS, La R.S. 17:3914 allows for Local Educational Agencies to contract with a private entity for student and other educational services and release personally identifiable information (PII), pursuant to the terms of the Contract,

WHEREAS, the Louisiana Department of Education (LDOE) and the Louisiana Division of Administration, Office of Technology Services (OTS) (hereinafter referred to as "State") acknowledge that EDGEAR OF AMERICA INC (hereinafter referred to as "Contractor") has entered into a contractual arrangement to which the Contractor will provide services to Local Educational Agencies (LEAs).

WHEREFORE, the State and Contractor do enter into this Agreement subject to the terms and conditions as specified herein.

## 1. Local Educational Agencies Stipulation

The Contractor acknowledges that local educational agencies (LEAs) in Louisiana submit student data directly to the Contractor. The Contractor hereby agrees to be bound, vis-à-vis any and all such Louisiana LEAs that unilaterally sign an addendum to this data sharing agreement, by all of the provisions of this Agreement with respect to any student data provided directly to the Contractor by such Louisiana LEAs.

## 2. Purpose of the Disclosure

The Contractor agrees to collect and use any data disclosed to it pursuant to this Agreement solely for the purposes of providing access to the data stored in the Special Education Reporting data system (eSER/SER) to the LEAs for download into their local data system. The LDOE via OTS will provide the Contractor access to a LEA's eSER/SER data via a secure, nightly data extract.

## 3. Data

OTS agrees to provide the Contractor with access to the respective LEA's eSER/SER student-level data contained in Appendix A. The LDOE will not have access to any student personally identifiable data.

The State and LEAs reserve the right to withhold any of the foregoing data if determined, in their sole discretion, that disclosure of such data would violate any provision of state or federal law.

## 4. Confidentiality

This Agreement is entered into by Contractor and the State in accordance with the provisions of the Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232(g), et seq., (FERPA) and La. R.S. 17:3914. The Contractor hereby acknowledges that all documents which include information contained in or derived from a student's education records are deemed confidential pursuant to FERPA and La. R.S. 17:3914 and therefore will not be disclosed by Contractor to any third party. Contractor further acknowledges that information contained in or derived from a student's education records are classified as "Restricted Data" by the State's Information Security Policy and are subject to the confidentiality requirements disclosed therein.

Contractor shall retain the original version of the data at a single location and shall not make a copy or extract of the data available to anyone except personnel who have a need for the data to perform the services referenced in this Agreement. Contractor shall maintain the data in hard copy or electronic form, in an area that has limited access only to Contractor's authorized personnel. Contractor shall not permit removal of the data from the limited access area. Contractor will ensure that access to the data maintained on computer files or databases is controlled by password protection. Contractor shall establish procedures to ensure that the target data cannot be extracted from a computer file or database by unauthorized individuals. Contractor shall maintain all printouts, discs, or other physical products containing student-level data in locked cabinets, file drawers, or other secure locations when not in use. Contractor shall, under supervision of the State, destroy the data provided to Contractor, including all copies, whether in electronic or hard copy form, when the services are completed or this Agreement is terminated, whichever occurs first. Encryption shall be utilized for the transport and storage of shared Confidential and Restricted Data in accordance with the State's Information Security Policy.

## 5. Restrictions on Use

Contractor shall not use the data for any purpose not expressly permitted in this Agreement. Contractor cannot disclose any document, whether in hard copy or electronic form, or otherwise disclose to any third party any student-level data or information in any form whatsoever or under any circumstances which would directly or indirectly make a student's identity traceable.

## 6. Indemnification

Contractor shall defend, indemnify and hold harmless the State and any and all of the State's directors, officers, officials, employees, agents, contractors and representatives against and from any and all costs, expenses, damages, injury or loss, including reasonable attorney's fees, to which they or any of them may be subject from any claims to the extent (i.e., for that portion) arising out of or related to Contractor's negligence, gross negligence or intentional misconduct or Contractor's breach of its obligations under this Agreement. For the avoidance of doubt, Contractor is not liable for any claims to the extent attributable to the fault or negligence of the State or its directors, officers, officials, employees, agents, contractors and representatives.

Contractor shall defend, indemnify and hold harmless any LEA and any and all of the LEA's directors, officers, officials, employees, agents, contractors and representatives against and from any and all costs, expenses, damages, injury or loss, including reasonable attorney's fees, to which they or any of them may be subject from any claims to the extent (i.e., for that portion) arising out of or related to Contractor's negligence, gross

negligence, or intentional misconduct or Contractor's breach of its obligations under this Agreement. For the avoidance of doubt, Contractor is not liable for any claims to the extent attributable to the fault or negligence of any LEA or their respective directors, officers, officials, employees, agents, contractors and representatives.

## 7. Ownership

Any data delivered or transmitted to the Contractor by the State and/or obtained or prepared by Contractor for the State pursuant to this Agreement shall become the property of the State, and shall, upon request, be provided or returned by Contractor to the State.

Any data delivered or transmitted to the Contractor by an LEA and/or obtained or prepared by Contractor for an LEA pursuant to this Agreement shall become the property of the LEA, and shall, upon request, be provided or returned by Contractor to the LEA. Any documents, materials, and/or products created or developed by Contractor under this Agreement for an LEA shall be the property of the LEA.

No records, reports, documents, materials or products created or developed under this contract can be distributed to third parties.

## 8. Security Audits

Pursuant to in La. R.S. 17:3914, the Contractor shall permit security audit checks pertaining to Contractor's security and usage of student data. Contractor shall cooperate with all security audits. Access shall be made available at all reasonable times on working days during working hours at Contractor's business premises to Contractor's employees, together with records, books and correspondence and other papers and documentation or media of every kind in possession of Contractor and Contractor's employees and directly pertaining to Contractor's services provided under this Agreement. No person or entity will access PII except as authorized by law.

## 9. Security Breach

As used in this Agreement "Security Breach" means any act or omission that compromises either the security, confidentiality or integrity of student information or the physical, technical, administrative or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality or integrity of personally-identifiable student information, or receipt of a complaint in relation to the privacy practices of Contractor or a breach or alleged breach of this Agreement relating to such privacy practices.

Contractor shall take commercially reasonable steps and best efforts, in accordance with industry standards, to prevent security breaches. Contractor shall also take commercially reasonable steps, in

accordance with industry standards, to immediately remedy any security breach and prevent any further security breach at Contractor's expense in accordance with standard industry practices and applicable law. Furthermore, Contractor's personnel shall comply with all security regulations in effect at the State's premises, the Information Security policy detailed in Attachment I, and externally for materials and property belonging to the State or to the project.

Contractor shall: (i) provide the State and LEA with the name and contact information for an employee of Contractor who shall serve as the State's and LEA's primary security contact and shall be available to assist State twenty-four (24) hours per day, seven (7) days per week as a contact in resolving issues and fulfilling obligations associated with a security breach; (ii) immediately notify the State and LEA via email, SMS text, or a phone call to the State and LEA contacts which have been provided to the Contractor once the Contractor becomes aware of a security breach; and (iii) report to the OTS Information Security Team (IST) any known Data Breach or Security Event, as defined in the OTS Information Security Policy, no later than forty-eight (48) hours after confirmation of the event. Notify the IST by calling the Information Security Hotline at 1-844-692-8019 and emailing the security team at infosecteam@la.gov.

Immediately following Contractor's notification to the State and LEA of a security breach, Contractor, the State, and the LEA shall coordinate with each other to investigate the security breach. Contractor agrees to fully cooperate with State and LEA in their handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing physical access to the facilities and operations affected; (iii) facilitating interviews with Contractor's employees and others involved in the matter; (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law or industry standards and as otherwise required by the State and LEA; and (v) providing any notices to persons or organizations affected by the security breach as required by law and as required by the State or LEA.

## 10. Terms of Agreement

Unless earlier terminated in accordance with this Agreement, this Agreement shall begin on May 17, 2023 and shall terminate on May 17, 2028. The effective date of this Agreement may be extended only if an amendment to that effect is duly executed by the parties and approved by the necessary authorities prior to said termination date. If either party informs the other that an extension of this Agreement is deemed necessary, an amendment may be prepared by one party for appropriate action by the other party.

## 11. Termination for Convenience

The State may terminate this Agreement at any time by giving Contractor and all LEAs written notice of such termination. Contractor may terminate this Agreement upon thirty (30) days advance written notice by giving the State and all LEAs written notice of such termination. Further, Contractor may terminate this Agreement at any time upon written notice with respect to the State or any LEA(s) if Contractor believes, in its reasonable discretion, that such party is not complying with applicable law with respect to eSER/SER student-level data. The Contractor must notify the State in writing within 24 hours if the contracted services with a school system participating in this agreement are terminated.

## 12. Assignment of Contract

Contractor shall not assign any interest in this Agreement by assignment, transfer, or novation, without prior written consent of the State. Nothing in this provision shall preclude the Contractor from subcontracting with third parties to perform work contemplated herein; however, the Contractor is responsible for ensuring that any such subcontractor(s) adhere to, and agree to be bound by, all provisions of this Agreement, and that any contract with such subcontractor(s) shall explicitly make such subcontractor subject to the audit provisions contained herein.

## 13. Jurisdiction, Venue and Governing Law

Exclusive jurisdiction and venue for any and all suits between the State and Contractor arising out of, or related to, this Agreement shall be filed and adjudicated in the 19th Judicial District Court, Parish of East Baton Rouge, State of Louisiana.

Exclusive jurisdiction and venue for any and all suits between the LEA and Contractor arising out of, or related to, this Agreement shall be filed and adjudicated in the appropriate Louisiana State District Court, in the Parish in which the LEA is domiciled.

Exclusive jurisdiction and venue for any and all suits among the Contractor, the State, and one or more LEAs arising out of, or related to, this Agreement shall be filed and adjudicated in the 19th Judicial District Court, Parish of East Baton Rouge, State of Louisiana.

The laws of the State of Louisiana, without regard to Louisiana law on conflicts of law, shall govern this Agreement.

## 14. Survival

Contractor's obligation under Clauses 2, 4, 5, 6, 7, and 13 shall survive expiration and/or termination of this Agreement. Contractor's obligations under Clauses 8 and 9 shall survive expiration and/or termination of this Agreement until Contractor has fully complied with its obligation to destroy data as set forth herein.

*IN WITNESS WHEREOF*, the parties have executed this Agreement as of the dates indicated below.

DocuSigned by:
Cade Brumley
B662C8EEAEBD74C3...

Dr. Cade Brumley,
State Superintendent of Education

2/5/2024
Date

DocuSigned by:
Derek Williams
6EDEB93D1FD14E7...

Louisiana Division of Administration,
Office of Technology Services
Derek Williams
State Chief Information Officer

2/8/2024
Date

DocuSigned by:
Keith Bores
ED9A44f9624B4...

EdGear of America, Inc.
Keith Bores
Operations Manager

2/5/2024
Date

# APPENDIX A

This document details each block that is in the nightly LEA export. Each block has the name, type, and length of all the attributes that are in the block.

- StudentBlock
- ParentGuardianBlock
- JurisdictionBlock
- SpedActivityBlock
- PostSchoolTransitionBlocks
- PrereferralActivityBlock
- ScreeningBlocks
- InitialEvaluationBlock
- ReevaluationBlock
- IepBlock
- ServicesPlanBlock
- ServiceBlock
- EsypEligibilityBlock

Student Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| StateIDNumber | numeric | 10 |
| LegacyStateIDNumber | numeric | 9 |
| First Name | alpha | 15 |
| Middle Name | alpha | 15 |
| Last Name | alpha | 20 |
| Suffix | numeric | 2 |
| Birth Date | numeric | 8 |
| EthHispanic | numeric | 1 |
| EthAmerIndianAlaskan | numeric | 1 |
| EthAsian | numeric | 1 |
| EthBlack | numeric | 1 |
| EthHawPacIslander | numeric | 1 |
| EthWhite | numeric | 1 |
| Gender | numeric | 2 |
| Dominant Language Code | numeric2 | |
| Current Grade Code | numeric | 2 |
| Iep Authority SSN | numeric | 9 |

Parent Guardian Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |

| | | |
|---|---|---|
| Title | numeric | 2 |
| First Name | alpha | 50 |
| Middle Name | alpha | 50 |
| Last name | alpha | 50 |
| Suffix | numeric | 2 |
| Address | alpha | 100 |
| City | alpha | 50 |
| StateCode | numeric | 2 |
| ZipCode | numeric | 5 |

Jurisdiction Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| LeaCode | alphanumeric | 3 |
| BeginDate | numeric | 8 |
| EndDate | numeric | 8 |
| LocalID | alphanumeric | 10 |
| SiteID | alphanumeric | 6 |

Special Ed Activity Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| EntryDate | numeric | 8 |
| Exit Date | numeric | 8 |
| Exit Code | numeric | 2 |
| ReEvaluationDeclineDate | numeric | 8 |

Post School Transition Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| SpecialEducationActivityExitDate | numeric | 8 |
| TypeCode | numeric | 2 |
| CareerCode | numeric | 2 |
| ContactCode | numeric | 2 |
| LivingArrangementCode | numeric | 2 |
| PostSecondaryCode | numeric | 2 |
| PlanToWorkFlag | numeric | 1 |
| WorkEnvironmentCode | numeric | 2 |
| WorkTypeCode | numeric | 2 |

Post School Transition Recreation Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| SpecialEducationActivityExitDate | numeric | 8 |
| PostSchoolTransitionTypeCode | numeric | 2 |
| RecreationCode | numeric | 2 |

Post School Transition Agency Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| SpecialEducationActivityExitDate | numeric | 8 |
| PostSchoolTransitionTypeCode | numeric | 2 |
| AgencyCode | numeric | 2 |

Student Referral Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| SblcEntryDate | numeric | 8 |
| ImmediatePreReferralReasonCode | numeric | 2 |
| SblcDecisionDate | numeric | 8 |
| SblcDecisionCode | numeric | 2 |
| RequestGradeCode | numeric | 2 |
| SurrogateParentNeededFlag | numeric | 1 |
| SurrogateParentAssignedDate | numeric | 8 |
| SurrogateParentNeedEndDate | numeric | 8 |
| TransitionPartCFlag | numeric | 1 |
| TransitionMeetingNoticeReceivedDate | numeric | 8 |
| TransitionMeetingDate | numeric | 8 |

Student Referral Reason Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| Entry Date | numeric | 8 |
| ReasonCode | numeric | 2 |

Screening Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| ScreeningDate | numeric | 8 |
| ScreeningCode | numeric | 2 |
| ScreeningResultCode | numeric | 2 |

Initial Evaluation Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestDate | numeric | 8 |
| ReportDisseminatedDate | numeric | 8 |
| EligibilityDeterminationDate | numeric | 8 |
| CoordinatorTitleCode | numeric | 2 |
| StaffMemberStateID | alpha | 10 |
| DecisionDate | numeric | 8 |
| DecisionCode | numeric | 2 |
| PrimaryExceptionalityCode | numeric | 2 |

Initial Evaluation Primary Exceptionality Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| EvaluationPermissionRequestDate | numeric | 8 |
| ExceptionalityDetailCode | numeric | 2 |

Initial Evaluation Secondary Exceptionality Block
Initial Evaluation Exceptionality Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ExceptionalityCode | numeric | 2 |

Initial Evaluation Exceptionality Detail Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ExceptionalityCode | numeric | 2 |
| ExceptionalityDetailCode | numeric | 2 |

Initial Evaluation Result Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| InitialEvaluationPermissionRequestDate | numeric | 8 |
| AltAssessmentTypeCode | numeric | 2 |
| AltAssessmentComplete | numeric | 1 |
| AltAssessmentCode | numeric | 2 |
| AltAsessmentOther | alphanumeric | 100 |
| AltAssessmentDate | numeric | 8 |
| StandardDeviation | alpha | 5 |
| RespondentCode | numeric | 2 |

Initial Evaluation Participant Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ParticipantCode | numeric | 2 |

Initial Evaluation Medical Impairment Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| MedicalImpairmentCode | numeric | 2 |

Initial Evaluation Extension Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ExtensionCode | numeric | 2 |

Reevaluation Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ReEvaluationReasonCode | numeric | 2 |
| ReportDisseminatedDate | numeric | 8 |
| CoordinatorTitleCode | numeric | 2 |
| StaffMemberStateID | alpha | 10 |
| PrimaryExceptionailtyCode | numeric | 2 |
| WaiveReEval | numeric | 1 |

Reevaluation Primary Exceptionality Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| EvaluationPermissionRequestDate | numeric | 8 |
| ExceptionalityDetailCode | numeric | 2 |

Reevaluation Secondary Exceptionality Block
Reevaluation Exceptionality Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |

| | | |
|---|---|---|
| PermissionRequestStartDate | numeric | 8 |
| ExceptionalityCode | numeric | 2 |

Reevaluation Exceptionality Detail Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ExceptionalityCode | numeric | 2 |
| ExceptionalityDetailCode | numeric | 2 |

Reevaluation Result Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| InitialEvaluationPermissionRequestDate | numeric | 8 |
| AltAssessmentTypeCode | numeric | 2 |
| AltAssessmentComplete | numeric | 1 |
| AltAssessmentCode | numeric | 2 |
| AltAsessmentOther | alphanumeric | 100 |
| AltAssessmentDate | numeric | 8 |
| StandardDeviation | alpha | 5 |
| RespondentCode | numeric | 2 |

Reevaluation Participant Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ParticipantCode | numeric | 2 |

Reevaluation Medical Impairment Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| MedicalImpairmentCode | numeric | 2 |

Reevaluation Extension Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| PermissionRequestStartDate | numeric | 8 |
| ExtensionCode | numeric | 2 |

Iep Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| TeamMeetingDate | numeric | 8 |
| CurrentGradeCode | numeric | 2 |
| TypeCode | numeric | 2 |
| ParentSignDate | numeric | 8 |
| ParentDecisionCode | numeric | 2 |
| PlacementDeterminationCode | numeric | 2 |
| CreatedDate | numeric | 8 |
| ModifiedDate | numeric | 8 |
| IsSubmitted | alpha | 3 |

Iep Service Plan Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| TeamMeetingDate | numeric | 8 |
| PlacementServiceDeterminationCode | numeric | 2 |
| TypeCode | numeric | 2 |
| ParentSignDate | numeric | 8 |
| ParentDecisionCode | numeric | 2 |
| CreatedDate | numeric | 8 |
| ModifiedDate | numeric | 8 |
| IsSubmitted | alpha | 3 |

Services Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| ServiceCode | numeric | 2 |
| StartDate | numeric | 8 |
| TerminationCode | numeric | 2 |
| TerminationDate | numeric | 8 |

Service Provider Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| ServiceServiceCode | numeric | 2 |
| ServiceStartDate | numeric | 8 |
| StaffMemberStateID | alphanumeric | 10 |
| ServiceDetailCode | numeric | 2 |
| ServiceLocationCode | numeric | 2 |

ESYS Block
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| BeginSchoolYear | numeric | 8 |
| EndSchoolYear | numeric | 8 |
| BeginDate | numeric | 8 |
| EndDate | numeric | 8 |
| ExitReasonCode | numeric | 2 |
| IepDecisionCode | numeric | 2 |
| EligRegression | numeric | 1 |
| EligCritical1 | numeric | 1 |
| EligCritical2 | numeric | 1 |
| EligEmployment | numeric | 1 |
| EligTransitionPartB | numeric | 1 |
| EligTransitionPostSchool | numeric | 1 |
| EligExcessive | numeric | 1 |
| EligExtenuating | numeric | 1 |
| NumberMinutesPerDay | numeric | 4 |
| NumberDays | numeric | 3 |
| TransportationCode | numeric | 2 |

ESYS Progress Report
BLOCK FORMAT

| | | |
|---|---|---|
| BlockID | alpha | 5 |
| EsypBeginSchoolYear | numeric | 4 |
| InstructionalPlanNumber | numeric | 4 |
| ProgressGoalType | numeric | 2 |
| ReasonType | numeric | 2 |

Student Testing Accommodations – future variable to be added to eSER

## ATTACHMENT I - STATE OF LOUISIANA INFORMATION SECURITY REQUIREMENTS

This attachment provides the additional information security requirements in addition to the existing Contract, Statement of Work, Data Sharing Agreement, and the other associated attachments.

## SAFEGUARDING CONFIDENTIAL AND RESTRICTED INFORMATION

The Contractor shall implement and maintain administrative, technical, and physical safeguards designed to protect against unauthorized access to or use of Confidential or Restricted Information received from, or on behalf of, the State by the Contractor pursuant to the performance of the agreed upon Services. For purposes of this attachment, Confidential Information includes Restricted Information. Restricted Information is data that requires strict adherence to legal obligations such as federal, state, or local law or required by State policy and so designated. Examples of Restricted Information include, but are not limited to: Protected Health Information (PHI), Federal Tax Information (FTI), Payment Card Information (PCI), Criminal Justice Information (CJI), and Personally Identifiable Information (PII) or data specifically designated by State as Restricted Information. The Contractor currently maintains the following:

- An information security program that defines implements, and reviews information security policies and procedures.
- Policies that prohibit the unauthorized disclosure of Confidential and Restricted Information and requesting, on an annual basis, confirmation from Contractor personnel that they have read such policies.
- Processes to encrypt Confidential Information stored on Contractor-provided laptop and desktop computers (using BitLocker Drive Encryption – full disk encryption); processes and security settings to protect Confidential Information stored on Contractor-provided mobile devices (e.g., iPhone and Androids), such as timeout values, PINs, automatic device wipe after a specified number of invalid log-on attempts, and remote wipe capability; and issuing encrypted USB drives to Contractor personnel for use in transferring Confidential or Restricted Information.
- Training and awareness programs for personnel related to information security policies, information protection standards, and privacy. Additionally, from time to time, publishing privacy and security-related alerts or reminders by standard Contractor internal communication channels.
- Limiting physical access to Contractor offices through the use of one or more of the following: conventional locks, electronic locks, security guards, identification badges, visitor control programs, and video surveillance programs.
- Anti-virus / Endpoint Detection and Response protection programs (e.g., Crowdstrike), including, centrally managed, commercially available anti-virus software on Contractor-provided computers to which updates are released as they become available from anti-virus software vendors, and a virus containment process that defines responsibilities and outlines procedures.
- Contractor-owned or operated network servers in the Contractor's data centers, co-located in a third-party data center or cloud environment, and/or deployed as contractor-owned and/or managed on-premise servers must employ a variety of industry-accepted procedures and tools that are designed to safeguard portions of the network and servers within the data centers. These include combinations of the following:

  - Restricting both physical and network access to authorized users
  - Restricting physical access by card-key control systems
  - Network-based intrusion prevention system
  - Firewalls to segment networks
  - Vulnerability assessment processes and tools
  - Change management procedures
  - Patch management processes and tools
  - Periodically backing up data that is maintained on Contractor network servers, including processes to encrypt backup media and to store backup media off-site
  - Server operating system hardening as appropriate
- Periodic review and update of internal Contractor information security policies and procedures.
- Incident Response processes containing escalation procedures for contacting State and Information Security resources.
- Sanitization of any decommissioned or inoperable Contractor-owned machine, storage, media, disk, or drive containing any Confidential or Restricted Information uses the following approved sanitization methods:

  Sanitization is divided into three types.

  Type 1, Clearing:

  Clearing an electronic storage media is the lowest level of sanitization that inhibits the recovery of information assets via a robust keyboard attack using data recovery tools. The use of conventional operating system utilities like deleting files or disk formatting only deletes the respective directory entries and thus does not inhibit the ability of data recovery tools to retrieve the information assets as the respective data itself is not being overwritten.

  Type 2, Purging:

  Methods of purging are:
  1. Wiping: Overwriting all locations including remapping bad sectors on a rewritable electronic storage media multiple times with different patterns, thereby checking the appropriateness by comparing different locations before and after overwriting. Required technology detail: The necessary number of overwrites, patterns, and location checks, which depend on the type of re-writable electronic storage media.
  2. Secure Erasing: Overwriting all locations on an ATA hard disk drive (a specific type of electronic storage media that includes PATA and SATA drives) a single time in a reliable manner. The Security Erase Unit command of the ATA specification must be used to initiate secure erasing. If implemented in a specific ATA hard disk drive, the Enhanced Erase Mode should be used. Successful execution must be checked afterward.
  3. Degaussing: Deleting all information assets stored on a magnetically sensitive electronic storage media using a strong magnetic field.
  4. Resetting: Returning a volatile electronic storage media into its initial delivery state. The power must be switched off and the backup battery removed if battery backed.

Type 3, Destruction:

Physically destroying electronic storage media is the highest level and thus the ultimate form of sanitization. Physical destruction is achieved when no portion of an electronic storage media can be used to extract a significant amount of data. Therefore, simply punching holes – for example into a hard disk – is not sufficient for physical destruction.

Methods of destroying are:

1. Shredding: Breaking an electronic storage media into parts. Disintegrating can be used as a synonym term for shredding. Required technology detail: The maximum size of the parts, depends on the type of electronic storage media.
2. Pulverizing: Crushing an electronic storage media into dust or powder.
3. Melting: Heating an electronic storage media past its melting point transforming it into a molten mass. The necessary melting point depends on the instance of the electronic storage media.
4. Incinerating: Burning an electronic storage media past its firing temperature transforming it into ash, flue gasses, and particulates. The necessary firing temperature depends on the instance of the electronic storage media.

The sanitization method and procedures selected by the Contractor must generate the appropriate unit-level logging as described below:

Each Sanitization Log Record must contain the following fields of information:

- Media or Device Type
- Sanitization Status Code
- Manufacturer unique ID (Ex. Hard drive Serial Number)
- Date and Time of Sanitization
- Full Name of individual that performed the sanitization

A certificate of destruction shall be provided if requested by the State.

## ACCESSING STATE NETWORKS, SYSTEMS, AND INFORMATION

Access to State resources requires the following: Contractor personnel connecting to State computing systems and resources shall only be in the performance of the agreed upon Services.

- Contractor personnel **shall not** knowingly (unless otherwise expressly agreed to by the parties as a function of the Services, or authorized in writing by the State's Information Security Team):
    - Access or attempt to access the State's Confidential or Restricted Information for any purpose outside of the scope of such Services.
    - Connect personal (i.e., non-work related or Contractor-provided) devices to the State's network.

- Attempt to alter or circumvent any State security controls safeguarding the State's network (e.g., authentication processes, access controls, firewall controls, web site blocking controls, etc.).
- Install, execute, or modify software, equipment, or peripherals on (or remove software, equipment, or peripherals from) the State network.
- Install or disseminate malicious code (including computer viruses, worms, and Trojan horses) on the State network.
- Conduct discovery or vulnerability scans of State networks, applications, or computing systems.
- Share or disclose any access code or password provided by, or generated on behalf of, the State to Contractor personnel for such access.

- Contractor-provided computer workstations or laptops used to access the State's data, computing systems, and resources will:
  - have commercial anti-virus / EDR software installed and configured to automatically signature updates released from the anti-virus software vendor while such computers are connected to Contractor's network or alternatively, if The Contractor's personnel does not connect their computers to the Contractor's network over a certain period of time, while such computers are connected to the Internet.
  - have security software patches installed on such computers, which patches, by the determination of Contractor's Information Security Office, are reasonably necessary to safeguard such computers from access by unauthorized third parties or from outside threats to the integrity and confidentiality of information residing on such computers.
  - have firewall software installed and operating on such computers while such computers are connected to the Internet.
  - have access controls designed to restrict access to such computers to authorized individuals.
  - have 128-bit (or better) AES file-level encryption enabled, which is configured to automatically verify encryption status.
  - have an automatic daily back-up of standard directories and files.
- All Contractor personnel shall review the terms and requirements of this attachment before accessing any State resources.
- If required, The State will provide Virtual Private Network (VPN) access to Contractor personnel for them to perform development, testing, and production support activities in a timely manner.
- The Contractor shall submit an access request for all resources requiring access to State resources. Access requests shall minimally contain:
  - Full Name of Contract Resource
  - Assigned Job Title
  - Physical Location (City, State, Country of resource's current Contractor office)
  - Specific System and Application Access Required (System, Application, or Database)
  - Tentative End of Contract Date (to be extended as needed via additional notification)
  - Remote Access Required (yes or no)
- All Contractor personnel must safeguard Confidential and Restricted information in accordance with the requirements described in this attachment.

- The State's Information Security Team will review all Contractor access requests and provide approval prior to Contractor personnel being granted access. In the event the Contractor's access request is denied, the State's Information Security Team will provide written justification for review by the Contractor.
- Contractor personnel accessing State resources and/or data outside of the United States are strictly prohibited from accessing Restricted Information (directly or indirectly) contained within any application, system, database, or device unless prior written approval is provided by the State's Information Security Team and Agency assigned Data Owner.

## DATA MANAGEMENT

- The State will provide Contractor personnel with access to Restricted data except as set out in the applicable SOW or otherwise requested in writing by the Contractor-assigned Project Manager and as allowable by law. (This may include, for example, requesting access to the State production environment for investigating potential defects identified during the Warranty Period.) For development and testing purposes, State will provide the Contractor personnel with de-identified data that is representative of production data but that does not contain PII data.
- State agrees:
- to disclose any PII or other applicable Restricted Information to Contractor, if such disclosure would not violate any applicable law, rule, or regulation.
- not to request the Contractor to use or disclose PII or other applicable Restricted Information in any manner that would not be permissible under any applicable law, rule, or regulation, if such use or disclosure were done by the State.
- to disclose to Contractor only the minimum amount of PII data (if any) reasonably necessary for Contractor to perform agreed upon Services under the applicable SOW.
- Agreed upon Services may require system testing to be performed in non-production environments that are utilized by the Contractor. Testing is controlled through the usage of de-identified or "mock data". "Mock Data" is data created by the Contractor and does not contain PII, or similarly regulated Restricted Information.
- If requested by the State, the Contractor may be authorized to perform the de-identification of production Restricted Information utilizing a State-approved documented process and a State-owned workstation. This type of de-identification request must be processed through The Office of Technology Services.
- The Contractor shall implement security measures such that non-production environments under Contractor's full control, do not contain Restricted Information unless provided with written authorization from the State's Information Security Team as an exception. If the State has access to enter data, the State is responsible for such data entry to not contain Restricted Information, such as in the UAT or Training environments.
- The State will limit the Restricted Information it provides to the Contractor (or otherwise makes available to the Contractor) to only that which is reasonably necessary to allow the Contractor to provide the agreed-upon Services.
- If Applicable, the Contractor will provide the State with a list of Contractor personnel who are authorized to receive or have access to State resources (systems, applications, and databases). The Contractor will maintain and update the access lists as needed.

- Disclosure of Confidential or Restricted Information by State to Contractor shall utilize appropriate security measures by State, including data encryption, to maintain protection of Confidential or Restricted Information being transferred to Contractor by State, and as required by applicable information protection laws.
- The State will promptly notify the Contractor's Lead Engagement Partner in the event it becomes aware that Restricted Information has been disclosed to the Contractor inadvertently or otherwise.
- The State will be responsible for the State legacy systems required to integrate or share data with applications or systems within the scope of the agreed-upon Services, and shall not expose non-production environments to Restricted Information.

## SECURE DEVELOPMENT

When agreed-upon Services require the Contractor to develop or configure systems or applications, the Contractor is responsible (unless otherwise authorized in writing by the State's Information Security Team) for:

- Working with the State's Information Security Team to require additional application or system-specific Information Security requirements are captured and agreed upon prior to initiating development or technology implementation through the set requirement and design sessions. The State's Information Security Team shall actively participate in applicable requirement and design sessions and review such deliverables.
- Performing an Application Risk Assessment that will be presented to the State's Information Security Team prior to production implementation.
- Operationally embedding methods for testing and validating application and system security within the development process. The Contractor shall provide methods for all developers and testers to independently run both static and dynamic security testing as part of each development or test cycle.
- Requiring and validating that all input or files provided by the target end user is validated and filtered via server-side processes prior to processing in order to prevent code injection and improve data integrity.
- Requiring and validating all system-to-system or application-to-application communication requires industry-standard authentication and agreed-upon secure protocols.
- Requiring and validating authentication secrets (including, but not limited to: passwords) are not stored in clear text in any configuration file, source code (compiled or otherwise), or database.
- Requiring and validating web application user session state is dynamic and appropriately managed utilizing currently accepted industry standards, in order to successfully prevent an unauthorized individual from obtaining the ability to bypass authentication controls by "hijacking" a valid session.
- Requiring applications integrate with the State's Microsoft Active Directory (AD) and Identity Management (IAM) solutions in such a way that internal State users seamlessly authenticate and are not presented with a logon form, if single-sign-on is applicable to the scope of the agreed upon Services and/or set out in the applicable SOW.
- Requiring application or system roles and permissions are managed by the State's AD and IAM solutions.
- Requiring and validating all applicable applications employ Transport Layer Security (TLS) version 1.2 or higher when transmitting Restricted Information.

## SECURE SYSTEM ADMINISTRATION AND MAINTENANCE

When agreed-upon Services require the Contractor to maintain or administer systems or applications, the Contractor is responsible (unless otherwise expressly agreed to by the parties as to being out-of-scope of the agreed-upon Services, set out in the applicable SOW or authorized in writing by the State's Information Security Team) for:

- Following the State's change management policies.
- Maintaining and renewing any applicable application security certificates before expiration.
- Testing and applying all applicable security patches or updates in a timely manner per the Work Plan.
- The State will test and apply applicable state-managed system or application security patches or updates in a timely manner.
- Requiring Systems utilize industry-accepted anti-virus / EDR as approved by the State's Information Security Team.
- Requiring Systems are restricted from connecting to the internet directly unless approved by the State's Information Security Team.
- Requiring and validating Systems and applications are configured or modified to produce the adequate baseline level of audit records and security event logs.
- Requiring that local accounts and local authentication are not utilized unless provided approval by the State's Information Security Team.
- Requiring system access roles are provided by the State's AD and IAM.

## GENERAL REQUIREMENTS

- In the actual or reasonably suspected event the Contractor's personnel has materially violated the terms or requirements of this attachment, the State shall be entitled to take action to disable or prevent access to such Contractor personnel until the violation can be investigated and resolved. The State shall notify the Contractor PM within 8 hours and provide a written status of the violation and the estimated time of unavailable access. The Contractor agrees that access restrictions resulting from a Contractor's personnel's actual or reasonably suspected material violation of the terms or requirements of this attachment causing delay or cost for the Contractor will not increase the cost of Services for the State. In the event that the suspected event was not an actual violation, any such delay may require a change request to enable the Contractor to meet the work plan, and any SLAs not met due to the unavailability of access will be waived.
- System or Application vulnerabilities discovered by the State (or individuals designated by the State) shall be addressed by the Contractor in a timely manner, not to exceed 60 days, at no additional cost to the State.
- The Contractor shall work with the State's designated resources to produce any documentation required to facilitate an Audit (internal or external) of the State when needed, in an urgent manner. If the estimated effort is above 20 hours for the individual audit request, the State will process a change request to continue contractor support.
- In response to evolving technologies, industry standards, and marketplace expectations, from time-to-time Contractor may upgrade or modify the processes and controls that it is required to maintain hereunder. The Contractor shall not be in breach of this Agreement or any SOW as a result of any

such change, provided that such change does not materially diminish the overall level of information security afforded to Confidential or Restricted Information by the processes and controls described hereunder. Any change to technology or processes previously reviewed and approved by the State's Information Security Team requires appropriate notification and prior written approval from the State's Information Security Team in addition to the Contractor's documented validation and testing of the newly proposed technology or process.