SCHEDULE E

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Education Analytics, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

4. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

5. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

Education Analytics, Inc.

BY: _____ **DATED:** 07-06-2023

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at: http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, Or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;
    a. We are calculating teacher/school/district level growth scores and student learning objectives based on student pre and post test data.

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
    a. None hired for this project

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
    a. Upon termination of this project, EA shall destroy all confidential information obtained in connection with the services offered and the education data records. The data will be returned to client upon termination or expiration of this agreement, as per the client's requirements in the project agreement. All hard copies of personally identifiable data in the possession of EA will be securely destroyed using a data destruction process including shredding, and all electronic data will be purged from the EA network

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
   Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
   a. EA ensures that access to the data is restricted solely to staff who need such access to carry out the responsibilities of the project based on their role, and that such staff will not release such data to any unauthorized party as agreed by signing of EA's non-disclosure agreement. Access to all computer applications and data at EA are managed and authorized at every step using the Windows Active Directory user ID and high security password procedures. Key personnel working on client data have federal security clearance and have undergone human subjects training on handling data. EA requires all staff to sign confidentiality agreements prior to providing data access.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

education analytics

EDUCATION ANALYTICS DATA SECURITY PLAN

Education Analytics will follow the Data and Security Plan outlined in this document by implementing reasonable technical and physical security measures to ensure the confidentiality, integrity, and availability of confidential data. EA's security measures can be summarized as followed:

SUMMARY OF POLICIES

Secure Data Transfer and Data Storage Protocols: All confidential data are transferred using EA's secure file transfer solution. All client data in house is stored on EA's file and backup servers, with access controlled via Active Directory. Our facility is locked 24 hours a day, 7 days a week, and entry requires authentication using a key fob with unique codes for each user. Within the secured office suite, the server room storing network devices and secure servers is locked 24 hours a day, 7 days a week, and entry requires authorization using a key fob with unique codes for each user. More details on this topic can be found below.

Authorized Data Access and Data Destruction Policy: EA ensures that access to the data is restricted solely to staff who need such access to carry out the responsibilities of the project based on their role, and that such staff will not release such data to any unauthorized party as agreed by signing of EA's non-disclosure agreement. Access to all computer applications and data at EA are managed and authorized at every step using the Windows Active Directory user ID and high security password procedures. Key personnel working on client data have federal security clearance and have undergone human subjects training on handling data. EA requires all staff to sign confidentiality agreements prior to providing data access. Also, EA prioritizes the ongoing training of employees and authorized users about laws governing the usage of sensitive data including FERPA and other appropriate state laws. More details on this topic can be found below. EA agrees that data will remain the property of the client. To this effect, EA has a data destruction policy which ensures that the electronic data stored on the EA file and backup servers are destroyed within the contracted time frames.

IT System Security: All internal servers deployed at Education Analytics shall be managed by an operational group that is responsible for system administration. Approved server configuration guides shall be established and maintained by this operational group, based on business needs.

IT Network Security: EA's computer network storing the data ensures appropriate and secure data access by utilizing firewalls, an intrusion detection and prevention system and up to date anti-virus

subscribes to appropriate auto-update services and is also manually updated where necessary including but not limited to anti-virus and operating system updates. All confidential data is stored on our secure storage array using a redundant disk configuration and is encrypted at rest for maximum data breach protection. All confidential data will ONLY reside on the EA secure file server and can be accessed only using authorized credentials. EA staff do not download any confidential data to generic PCs (office or personal), laptops, or any removable storage device or mobile device. Data stored on our file servers are encrypted at the volume level with the AES-256 encryption standard with the encryption key available only to the technical administrators.

Physical Location Security of IT resources

Physical access to our facility is designed with intruder detection systems and requires personal authentication. Exterior doors to our location are monitored 24 hours a day, 7 days a week with surveillance cameras and are locked after business hours. Alarm systems installed on doors detect unauthorized access and alert appropriate authorities. Our office suite is locked 24 hours a day, 7 days a week and requires authentication using a key fob with unique codes for each user. The list of staff with access to the server room will continue to be reviewed quarterly against the number of times each staff gained access to the server room.

EA ensures that all content and applications of Education Analytics are maintained within the physical boundaries of the continental United States at all times, and all data processed, stored and maintained by EA within the scope of the agreement shall NOT leave the borders of the United States. The exact location details for all contents and applications can be provided upon request.

II. Authorized Data Access Policy

EA acknowledges that the individually identifiable data provided by clients are sensitive, requiring appropriate levels of security to prevent unauthorized disclosure or modification. EA will take all reasonable measures to protect the confidentiality of the data as required by federal and state laws and regulations applicable to EA. These may include but are not limited to the federal Social Security Act and Family Educational Rights and Privacy Act; internet security laws; and any regulations promulgated thereunder.

Data Security

EA acknowledges that it has full and final responsibility for the security of the data. EA agrees to implement reasonable technical and physical security measures to ensure the confidentiality, integrity, and availability of the data. EA's security measures may be reviewed by the client, both through an informal audit of policies and procedures and/or through inspection of security methods used within EA's infrastructure, storage, and other physical security. EA will review its implementation and maintenance of its security review periodically to protect the data in strict compliance with statutory and regulatory requirements.

External third-party access to sensitive institutional data shall be governed by contractual agreements: Access to sensitive client data by external parties shall be governed by individual contractual agreement with client and EA shall not transfer the data to any third party without client's prior approval.

Remote Access Policy

Windows Server remote access to users is provided for remote access to server resources secured using an SSL connection. To add security to these remote connections, the following guidelines are used:

- Use strong passwords
- Software kept up to date
- Access restrictions applied using firewalls
- Enabling Network Level Authentication
- Limit users authorized to access Remote Desktop
- Setting an account lockout policy

EA's internal password standards

Education Analytics (EA) employees and authorized users must adhere to the minimum password standards for all systems and applications that come into contact with EA resources.

To remedy password compliance issues, EA reserves the right to:

- Suspend access to preserve the confidentiality, integrity and availability of the network, systems or information;
- Periodically audit passwords for compliance; and
- Pursue disciplinary action because of non-compliance.

Absent a more secure password selection, the baseline password standard for users and owners of these systems is as follows:

- Passwords chosen must
    - be a minimum of seven (12) characters in length
    - be memorized or stored in EA's password management system
    - contain at least one (1) character from three (3) of the following categories:
        - Uppercase letter (A-Z)
        - Lowercase letter (a-z)
        - Digit (0-9)
        - Special character (~`!@#$%^&*()+=_-{}[]\|:;"'?/<>,.)
    - be private
- Windows domain user passwords expire every 90 days forcing users to reset their password to a new one different from the last five passwords used.

Data Security and Privacy Training- Increased Awareness of Securing Data Access and Transfer

EA prioritizes the ongoing training of employees and authorized users about laws governing the usage of sensitive data including FERPA and other appropriate state laws. All EA staff are expected to have their human subjects training certification active and this is continuously offered to EA staff on a regular basis.

- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.

Monitoring: All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental file level backups will be retained for at least 90 days.

Reporting: Security-related events will be reported to IT ticketing system, and IT helpdesk staff will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

IV. Computer Network and User Level Security: Firewalls, Security Scans, and Intrusion Detection solutions

Application layer vulnerability scans

EA's IT department does weekly, documented application layer security scans, (attack vectors, recommendations, etc.) and analyses and provides recommendations/generates work plans to remediate issues. This setup employs regular automated and fully reported scans which are reviewed weekly.

Operating system-layer vulnerability scans

Endpoint security software regularly monitors systems locally for irregularities, as well as offer perimeter scanning and filtering. Scans are conducted locally on a weekly basis on all files and logical system internals.

Intrusion Detection and Prevention System

An IDS/IPS system is provided by EA's next generation firewall. This system is designed to protect against known attack signatures and is kept up to date automatically as new signatures are added. The system also mitigates vulnerabilities by blocking traffic that does not conform to RFC standards and can prevent advanced evasion techniques. DoS and DDoS attacks are mitigated by enforcing rate limits on external services. Logs from the IDS/IPS system are stored for review and analysis.

Scenario 1: File, folders or collections of files and folders is accidentally deleted by a user

Solution: Restoration will be performed via latest available local backup set of data

Scenario 2: Failure of virtual server requiring rebuild or restoration

Solution: Restoration will be performed from virtual machine in full, from the latest available backup

Scenario 3: Failure of physical server requiring rebuild or restoration

Solution: Warranty repair of server will be done and then backup disks to temporary system will be mounted, & backups will imported and critical data restored to temporary location for immediate use

Scenario 4: Failure of network equipment

Solution: Reroute failed network connections to working equipment

Scenario 5: Ransomware/Cryptolocker Event

Solution: Address outbreak/infection issue and restore affected data from latest backup set

Scenario 6: EA office building is uninhabitable

Solution: Provided internet remains available, access to EA's computer network will be obtainable via remote portal/session host server.

Outage plan

Anticipated Outage Process: Outages are occasionally scheduled to allow the IT department to update and implement changes to infrastructure that cannot be done during production times due to potential conflicts to Usage, Accessibility and other service metrics. Standard monthly maintenance windows are scheduled for the first Friday of the month starting at 6pm CT and ending at 6am Sat morning. Changes to this scheduled outage, including requests for additional outages are reviewed and approved through the Operations-technology group. Once approval for outage is obtained, communication will be given to all affected userbases. This communication will provide the following:

- What: Summary of outage: Include client facing service name and brief description of outage or change.
- Why: Reason for outage or change. Why is this outage happening?
- When: Date, time and duration of proposed outage or change implementation window.
- Clients: If known, who and how many will be impacted.
- Risk elements: Testing results, training required, time to perform work, back-out/recovery plan, impact if change not performed.

protect the confidentiality of the Data as required by federal and state laws including but not limited to the federal Social Security Act and Family Educational Rights and Privacy Act; internet security laws; and any regulations promulgated thereunder. EA acknowledges that it will receive and/or come into contact with personally identifiable information, that directly relate to a student(s), teacher(s) or principal(s). EA will have in place sufficient protections and internal controls to ensure that the personally identifiable information from education records it receives is safeguarded in accordance with applicable laws and regulations and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records.

As mentioned above, EA shall limit internal access to education records to those individuals that are determined to have legitimate educational interests, not use the education records for any other purposes that those explicitly authorized by the project scope and shall maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and use encryption technology to protect data while in motion or in its custody from unauthorized disclosure. Also, EA shall:

- Identify the exclusive purposes for which the student data, or teacher or principal data, will be used
- Ensure subcontractors if any abide by data protection and security requirements
- When the agreement expires, ensure that subcontractors abide by data and security requirements
- Implement data storage and encryption solutions for storage and access of student, teacher, or principal data will be stored
- Abide by the policies and procedures outlined in the data security and privacy plan

VII. Security Audit process and Data Breach Policy

Audit process

EA provides the required IT resources to assist the client to conduct a security audit of EA's physical environment where IT resources including data and servers are located. The security audit process will cover the following steps to identify, evaluate and analyze potential threats and fixes for evaluating the security requirements of EA's IT system.

- Step 1: Information and technology asset identification and classification
- Step 2: Threat and vulnerability assessment of IT resources
- Step 3: Evaluation of controls
- Step 4: Analysis, decision, and documentation

Access to system security and data access audit logs on EA servers can be set up on client's request.

EA contracts with an external third party to perform IT audits every other year.

Data Breach Policy

In case of breaches to the student data or teacher or principal data, EA will activate its incident response plan upon a preliminary analysis of the incident. If incident response team activation is deemed appropriate, EA's cyber security and breach consultants will be notified. The breach coach (provided by the cyber security insurance provider) will act as a first responder and walk through what needs to

solutions. EA allows remote access only to authorized users using a remote gateway secured using SSL. More details on this topic can be found below.

IT Risk Management and Contingency Planning: EA has a disaster recovery plan and a process for handling outages which will be utilized in cases a need arises. EA has redundant and uninterruptible power and internet infrastructure provisions in place. In case of data breaches, EA will notify its cyber security insurance provider about the breach and work with the provider to investigate the breach and inform the related parties. More details on this topic can be found below.

Compliance with FERPA and Data Security Laws: EA is in strict compliance with data security and privacy laws including but not limited to FERPA, and ensures that its staff are trained on the required laws and kept up to date to gain knowledge about how to store, access and treat data records with a high level of security. More details on this topic can be found below.

Security Audit process and Data breach policy: EA's IT systems maintain incident, change management logs and allows for audits of the IT data security compliance. The security audit process will cover the following steps to identify, evaluate and analyze potential threats and fixes for evaluating the security requirements of EA's IT system. In case of breaches to the student data or teacher or principal data, EA will activate its Incident Response Team. This team will investigate the breach and notify the educational agency owning the data as necessary in accordance with regulations. EA will promptly comply with any inquiries from the client based upon the client's receipt of a complaint or other information indicating that improper or unauthorized disclosure of personally identifiable information may have occurred. More details on this topic can be found below.

Additional details on the above data security systems and processes can be found in the sections below:

I. Secure Data Transfer and Data Storage Protocols

Secure Data Transfer

Education Analytics takes great consideration to protect confidential data throughout the lifecycle of data use. Industry best practices, NIST security recommendations, as well as leaders in the field of educational data protections inform our organizational data policies. EA uses a secure file transfer solution for secure data transfer with clients. The secure file transfer solution uses state-of-the-art technology and industry best practices for data encryption during transit to and from the service as well as while stored within the host's servers. Information clients uploaded to and EA download from the transfer service are stored in our in-house dedicated EA secure file server which passes through appropriate firewalls and requires user authentications controlled by complex password requirements to prevent unauthorized access. Data hosted on the secure File transfer service servers is downloaded onto our secure local file server storage and any copy of the data on the file transfer host's server is periodically deleted to ensure highest form of security.

Secure Data Storage Server

All data received from clients are stored on dedicated EA secure Windows file servers stored in our locked server room inside our locked EA offices. The EA file server is configured for user authorizations and folder permissions using Windows Active Directory group membership services. The EA file server

Restricted Access

Access to the client data will be restricted solely to staff who need such access to carry out the responsibilities of the contractor under this agreement, and that such staff will not release such data to any unauthorized party. To protect against unauthorized data access, EA enforces the following practices:

- Role-based data access security policies
- Secure data storage servers
- Windows Active Directory based user credentials and complex password standards
- Provide staff data security and privacy trainings to create increased awareness of securing data access and transfer

Role based data access security policies

At the technical level, IT administrators craft auditing and role-based access policies for users based in Windows Active Directory. These policies are reviewed multiple times per year. Logon to user assigned workstations is limited to named users and access to data is provided on a need-to-know basis. Logon to servers is restricted to named operators in the Technical Services unit and disposal policies ensure that all data is removed from machines. Depending on the sensitivity of the data and the requirements of the data provider, we implement additional security policies at the group or sub-group level. These policies can be created to restrict access to storage areas or can limit the access of individuals to meet narrow security requirements.

Data Access Approval Process

System Administrators approve access to sensitive institutional data: Access to sensitive client data is approved by EA data administrators in accordance with the data release agreements signed with the client and in compliance with FERPA and appropriate state and federal laws. Access shall be granted only to EA employees, affiliates, and systems that need the access to perform the project.

Data administrators shall ensure that procedures for requesting and approving access to sensitive client data exist and are followed. Data administrators shall also implement procedures for regularly auditing access to sensitive client data and revoking access when it is no longer needed or authorized. All procedures shall include sufficient tracking for requests, approvals, and revocations such that authorized access to sensitive client data is auditable.

Only authorized users shall access sensitive client data and data users shall use sensitive institutional data responsibly: All access by individuals to sensitive institutional data shall be controlled by reasonable measures to prevent access by unauthorized users: Data users must responsibly use data for which they have access including only using the data for its intended purpose and respecting the data privacy. Data users must maintain the confidentiality data in accordance with all applicable laws including EA's Employee Confidentiality agreements. Authorized access to sensitive institutional data does not imply authorization for copying, further dissemination of data, or any use other than the use for which the employee was authorized. The data administrator retains the right to approve and grant access to sensitive institutional data.

These efforts focus on developing an awareness of how sensitive information are accessed, stored, and transferred.

Data Destruction, Purging and Archival policy

Upon termination of this project, EA and EA's subcontractors shall destroy all confidential information obtained in connection with the services offered and the education data records. The data will be returned to client upon termination or expiration of this agreement, as per the client's requirements in the project agreement. All hard copies of personally identifiable data in the possession of EA will be securely destroyed using a data destruction process including shredding, and all electronic data will be purged from the EA network.

III. IT Systems and Server Security

All internal servers deployed at Education Analytics shall be owned by an operational group that is responsible for system administration. Approved server configuration guides shall be established and maintained by this operational group, based on business needs. This operational group will monitor configuration compliance and implement an exception policy as needed and establish a process for changing the configuration guides, which includes review and approval by IT. More details on this topic can be found below. The following requirements must be met to be compliant with server security:

- For servers that are registered within EA's domain, at a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location.
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
    - Information in the IT management system must be kept up-to-date
    - Configuration changes for production servers must follow the appropriate change management procedures

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.

Configuration Requirements

- Operating System configuration should be in accordance with approved IT guidelines.
- Services and applications that will not be used should be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function and do not use root when a non-privileged account unless absolutely necessary.

V. IT Risk Management and Contingency Planning: Network Infrastructure, Redundant Power, Data Backups, Software Management and Disaster Recovery:

File level backups of the client data are performed every day. Backup copies are stored up to 365 days. The data volumes are backed up using Veeam backup solution on to our network attached storage through an iSCSI protocol on EA's internal network. EA administrators manage and audit the user accounts and actions as well as file logs.

Primary Site/disaster recovery location for data storage and site security

Primary data storage is located in EA's file servers in our physical office location in Madison, WI. Disk based backups are stored on-site on a separate storage appliance, and a local co-location facility may be used to for secure off-site backup storage. Backups replicated to this facility are done so asynchronously and are encrypted.

Internet connectivity

EA utilizes a minimum 100 MBPS symmetrical fiber circuit for primary internet connectivity with fail over capability offering a 99.99% SLA with remedies. The setup offers two redundant circuits with managed fiber/wireless redundancy offering SLA and uptime guarantees as mentioned above in practice and managing the failover piece on the ISP's end using BFD/OSPF/BGP. In a Loss of Service event affecting the primary WAN port, the firewall will automatically failover all WAN traffic to an Internet connection provided by a secondary carrier for temporary failover services. In an LOS event, the failover connection may provide limited bandwidth or functionality compared to the primary connection. The firewall is configured to fallback to the primary connection once an LoS event has ended and the primary WAN interface reports as being in an "up" state.

Redundant and Uninterruptible Power

EA's key systems including compute servers, storage servers, and network infrastructure are connected to uninterruptible power supplies (UPS). The UPS allows for sufficient time for key systems to be safely shut down using automatic or manual procedures.

Backup and Recovery plan

Infrastructure virtual machines (backend systems responsible for the operation of the network, security policies, computer configurations, network shares are all backed up via Veeam Backup & Recovery software to a separate backup storage device. Virtual machines are retained in backup on a 365-day basis. Project file level data is backed up daily on schedule to the same backup device as the VMs. File level data is retained for 30-365 days based on partner contract DRAs. Non-project file level backup is also provided by Veeam Backup & Recovery software and retained for up to 365 days.

In case of a situation that warrants disaster recovery, EA will opt for the recovery solution based on the scenario causing the disaster. The disaster recovery scenarios and solutions that EA utilizes are listed below.

Unanticipated Outage and Escalation Process: This is a process for communication and teamwork during an unplanned outage.

- Since unplanned outages require quick attention, all that is initially required is an immediate notification to users reporting the outage. Once the unplanned outage is resolved and service restored, a more detailed follow up shall be provided to users.
- All unplanned outages are considered incidents and an incident ticket in IT request will record the impact and status update of the outage.
- All subsequent documentation shall occur within the IT request ticket, including outage status updates and resolution once service has been restored.
- All subsequent communication to leadership and userbase should occur as necessary via the most appropriate venues to reach affected users (email, slack, phone, etc).

Software Remediation, Incident, Change and Release Management

For software defects present in purchased software products used by EA, the respective software products are updated to fix any defects as soon as the product conducts their QA and release fixes.

For incident management including data security incidents and outage incidents, incident logs shall be used for analyzing and determining plans for management.

For change management including widely affecting system changes, enhancements and other multi stepped changes, IT staff meet to define requirements, create deliverables and a stepped implementation plan which is shared with users throughout the implementation period. Details of the work performed, and any issues encountered, are fully documented in the IT ticket system before completion and retained in perpetuity for reference.

Release management: Releases of data security products used by EA such as antivirus solutions and coding solutions are monitored for and patches/updates of software releases are installed on a regular basis.

VI. Compliance with FERPA and Data Security Laws:

Education Analytics (EA) security guidelines outline the rights and responsibilities of users and makes clear the need for increased levels of security for research and administrative data through its responsible use, electronic devices, and password standards policies. EA requires each employee to sign the *Education Analytics Employee Confidentiality Agreement*. This agreement is for employees to understand and acknowledge their responsibilities to protect and safeguard the restricted use of confidential information. Employees and agents of EA will abide by the confidentiality provisions of the Family Educational Rights and Privacy Act (FERPA), 20 USC 1232g, 34 CFR 99, sec. 118.125 Wis. Stats., and low income information under the National School Lunch Act, 42 USC 1758(b)(2)(C)(iii) to (v). Also, all users are required to sign EA's *IT Appropriate Use Policy*. Additionally, EA requires that users of our networked system use a secure operating system that requires logon and provides file-level security.

EA will always ensure appropriate levels of security as described in the above sections to prevent unauthorized disclosure or modification of sensitive data. EA shall take all reasonable measures to

happen next. An outside IT consultant can be hired by the breach coach to come in and look for suspicious activity, data mine, or work with the breach consultant to determine next steps.

EA in collaboration with its breach consultant will notify the educational agency owning the data of any breach of security resulting in an unauthorized release of such data in accordance with implementing regulations. Upon such notification, the educational agency shall take appropriate action in accordance with any implementing regulations.

EA will cooperate and promptly comply with any inquiries from the client based upon the client's receipt of a complaint or other information indicating that an improper or unauthorized disclosure of personally identifiable information may have occurred. EA will permit on-site examination and inspection and will provide at its own cost necessary documentation or testimony of any employee, representative or assignee of EA relating to the alleged improper disclosure of data.

Updated 5/7/2021 - jdl