

STANDARD STUDENT DATA PRIVACY AGREEMENT

**MASSACHUSETTS, MAINE, ILLINOIS, IOWA, MISSOURI, NEBRASKA, NEW HAMPSHIRE,
NEW JERSEY, NEW YORK, OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA**

MA-ME-IL-IA-MO-NE-NH-NJ-NY-OH-RI-TN-VT-VA-NDPA, Standard Version 1.0

Manchester School District (SAU 37)

and

Stickball Inc.

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Manchester School District (SAU 37), located at 20 Hecker Street, Manchester, NH 03102 USA (the “**Local Education Agency**” or “**LEA**”) and Stickball Inc., located at 60 State St, Suite 1100, Boston, MA 02109 USA (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - ☒ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - ☒ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Sahal Laher Title: CEO

Address: 158 Endicott St Suite 4, Boston, MA 02113

Phone: 603-264-3127 Email: sahal@stickball.biz

The designated representative for the LEA for this DPA is:

Stephen Cross, Chief Information & Cyber Security Officer
20 Hecker Street, Manchester NH 03102
6036246300 scross@mansd.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Manchester School District (SAU 37)

By:  Date: 06/23/2025
STEPHEN CROSS (Jun 23, 2025 10:03 EDT)

Printed Name: Stephen P. Cross Title/Position: Executive Director of Technology

Stickball Inc.

By:  Date: 6-20-25

Printed Name: S. LAHER Title/Position: CEO

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit “F”**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “F”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA’s use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of

all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

Stickball, an interactive life-skills, financial-literacy, and workforce-readiness education, built with AI and immersive tools.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if Used by Your System
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	Single Sign On Module Progress (anonymized)
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input checked="" type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT “G”
Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act (“LRA”), 50 ILCS 205; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Illinois;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: “This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed.”
2. Replace Notices with: “Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.”
3. In Article II, Section 1, add: “Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.”
4. In Article II, Section 2, replace “forty-five (45)” with “five (5)”. Add the following sentence: “In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.”

5. In Article II, Section 4, replace it with the following: “In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.”
6. In Article II, Section 5, add: “By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).”
7. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
8. In Article IV, Section 6, replace the whole section with:

The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
10. In Article IV, Section 7, add “renting,” after “using.”

11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States, Canada, United Kingdom and/or the European Union.
12. In Article V, Section 4, add the following: “‘Security Breach’ does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.”
13. In Article V, Section 4(1) add the following:
 - vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
 - vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
14. In Article V, Section 4, add a section (6) which states:

In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

 - a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
 - b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
 - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

 - d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.
15. Replace Article VII, Section 1 with: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.”
16. In Exhibit C, add to the definition of Student Data, the following: “Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

student records", "student temporary record" or "student permanent record" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA."

17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E:
"The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."
18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
20. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.
22. The Provider will not collect social security numbers.

EXHIBIT “G”
Iowa

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Iowa. Specifically, those laws are Iowa Code §§ 22; Iowa Code §§ 715C, 281 I.A.C. 12.3(4); 41; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Iowa;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Iowa does not require all Student Data to be stored within the United States.
4. In Exhibit “C” add to the definition of “Student Data” significant information on progress and growth, experiences, interests, aptitudes, attitudes, abilities, part-time employment, and future plans.

EXHIBIT “G”

Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
 - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
 - i. Details of the incident, including when it occurred and when it was discovered;
 - ii. The type of personal information that was obtained as a result of the breach; and
 - iii. The contact person for Provider who has more information about the incident.
 - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
 - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
 - i. Social Security Number;
 - ii. Driver’s license number or other unique identification number created or collected by a government body;
 - iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - v. Medical information; or
 - vi. Health insurance information.

EXHIBIT “G”
Nebraska

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Nebraska. Specifically, those laws are Neb. Rev. Stat. Secs. 79-2,104; 79-2,153 to 79-2,155; 79-2, 539; 87-801 to 87-808; and 92 NAC 6; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Nebraska;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article II, Section 5, add, “Specifically, any written agreement with a Subprocessor will: (1) prohibit the Subprocessor from using Student Data any purpose other than providing the contracted service to or on behalf of the Provider; (2) prohibit the Subprocessor from disclosing any Student Data provided by the Provider with subsequent third parties; (3) and requires the Subprocessor to implement and maintain reasonable security procedures and practices.”
2. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
3. In Article IV, Section 4, replace: “Provider will not Sell Student Data to any third party” with “Provider will not Sell or rent Student Data to any third party.”
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Nebraska does not require data to be stored within the United States.

EXHIBIT "G"
New Jersey

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Jersey. Specifically, those laws are N.J. Stat. § 56:8-166.4 et seq.; N.J. Stat. § 18A:36-19; N.J. Stat. § 18A:36-19a; N.J. Stat. § 18A:36-35; N.J. Admin Code § 6A:16-7.9; N.J. Admin. Code § 6A:32-2.1; N.J. Admin. Code § 6A:32-7 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Jersey;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. The Provider will not disclose on its web site any personally identifiable information about a student, including, but not limited to student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
4. The Provider will not process Student Data in violation of State and federal laws that prohibit unlawful discrimination.
5. The Provider will not conduct processing that presents a heightened risk of harm to students without conducting and documenting a data protection assessment of each of its processing activities that involve Student Data.
6. In Article V, Section 1 Data Storage: New Jersey does not require data to be stored within the United States.
7. Add to the definition in Exhibit "C" of Student Data: "The location and times of class trips."

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
 - a. Location-tracking features of a school-issued device;
 - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
 - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT “G”
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student’s ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student’s requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq.*; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
 - a. Political affiliation;
 - b. Religion;
 - c. Voting history; and
 - d. Firearms ownership

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;
 - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
 - (4) Authorize wireless access prior to allowing such connections;
 - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
 - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
 - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
 - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
 - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
 - (10) Perform maintenance on organizational systems;
 - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
 - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
 - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
 - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
 - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
 - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit "G"

New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA’s Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor’s Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.
8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **“Exhibit D”**.

11. To amend Article IV, Section 7 to add: ‘Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, “which term shall not include students.”
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department’s Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider’s expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider’s privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
 - vi. The number of records affected, if known; and
 - vii. A description of the investigation undertaken so far; and
 - viii. The name of a point of contact for Provider.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency 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
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.
-

Exhibit “J”
LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es.

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at

See attached

INFORMATION SECURITY PROGRAM

Stickball Inc.

October 20, 2024

EXECUTIVE SUMMARY

This Information Security Program establishes a comprehensive framework for protecting Stickball Inc.'s information assets and technology infrastructure. As a cloud and AI-powered learning platform focusing on financial literacy and workforce readiness training, Stickball faces unique security challenges related to educational data, AI systems, and cloud infrastructure. This program defines the security controls, processes, and responsibilities designed to protect the confidentiality, integrity, and availability of information while enabling the business to operate efficiently and meet compliance requirements.

1. INTRODUCTION

1.1 Purpose and Scope

The purpose of this Information Security Program is to:

- Establish a security governance framework
- Define security roles and responsibilities
- Identify and protect critical information assets
- Implement appropriate security controls
- Ensure compliance with legal and regulatory requirements
- Create a security-aware culture
- Develop incident response capabilities
- Enable continuous improvement of security posture

This program applies to:

- All information assets regardless of format or location
- Technology infrastructure including cloud environments
- All employees, contractors, and third parties with access to Stickball systems
- Business processes that create, process, or store information
- Development and operations of the learning platform

- AI and machine learning systems

1.2 Security Principles

Stickball's Information Security Program is guided by the following principles:

- **Defense in Depth:** Multiple layers of controls to protect critical assets
- **Least Privilege:** Access limited to what is necessary for job functions
- **Separation of Duties:** Critical functions divided among different individuals
- **Risk-Based Approach:** Security resources focused on highest risks
- **Privacy by Design:** Privacy considerations built into systems and processes
- **Secure by Default:** Security embedded in systems from the beginning
- **Continuous Improvement:** Regular evaluation and enhancement of controls

1.3 Security Governance

1.3.1 Security Governance Structure

Executive Security Committee

- Composition: CEO, CTO, CISO, COO, Legal Counsel
- Responsibilities: Setting security strategy, approving policies, resource allocation
- Meeting Frequency: Quarterly

Security Steering Committee

- Composition: CISO (Chair), Dept. Heads, Security Team Leads
- Responsibilities: Program oversight, risk decisions, cross-functional coordination
- Meeting Frequency: Monthly

Security Working Groups

- Cloud Security Group
- Application Security Group
- Data Security Group
- AI Security Group
- Compliance and Risk Group

1.3.2 Key Roles and Responsibilities

Role	Primary Responsibilities
Chief Information Security Officer (CISO)	Overall security program, strategy, reporting to leadership
Security Operations Manager	Day-to-day security operations, monitoring, incident response
Cloud Security Architect	AWS environment security, cloud security controls
Application Security Lead	Secure development practices, application security testing
Data Security Lead	Data protection, encryption, privacy controls
Security Compliance Analyst	Regulatory compliance, security assessments, documentation
Security Awareness Coordinator	Training, awareness campaigns, behavior monitoring
All Employees	Following security policies, reporting incidents, security awareness

2. RISK MANAGEMENT

2.1 Risk Assessment Framework

2.1.1 Risk Assessment Methodology

Stickball follows a structured approach to security risk assessment:

1. **Asset Identification:** Inventory and classify information assets
2. **Threat Analysis:** Identify potential threats to assets
3. **Vulnerability Assessment:** Identify weaknesses in controls
4. **Impact Analysis:** Determine potential business impact
5. **Likelihood Determination:** Estimate probability of occurrence
6. **Risk Calculation:** Combine impact and likelihood
7. **Risk Prioritization:** Rank risks for treatment
8. **Risk Treatment:** Select and implement controls

2.1.2 Risk Rating Matrix

Impact	Description	Examples
Critical	Severe damage to organization	Data breach affecting thousands of users, extended platform outage
High	Significant damage	Localized data exposure, temporary service disruption
Medium	Moderate damage	Limited data exposure, minor functionality issues
Low	Minor damage	Isolated security event, minimal impact

Likelihood	Description	Frequency Estimate
High	Likely to occur	More than once per year
Medium	Possible occurrence	Once every 1-3 years
Low	Unlikely occurrence	Once every 3-5 years
Very Low	Rare occurrence	Less than once every 5 years

Risk Level Matrix

	Critical Impact	High Impact	Medium Impact	Low Impact
High Likelihood	Critical Risk	High Risk	Medium Risk	Low Risk
Medium Likelihood	High Risk	High Risk	Medium Risk	Low Risk
Low Likelihood	High Risk	Medium Risk	Medium Risk	Low Risk
Very Low Likelihood	Medium Risk	Medium Risk	Low Risk	Low Risk

2.2 Risk Assessment Process

2.2.1 Assessment Frequency

- Comprehensive risk assessment: Annual
- Critical system assessment: Semi-annual
- New system/application assessment: Prior to deployment
- Significant change assessment: Prior to implementation

- Third-party assessment: During vendor onboarding and annually

2.2.2 Key Risk Areas

- **Cloud Infrastructure Security:** AWS environment, configuration management
- **Application Security:** Learning platform, authentication systems, APIs
- **Data Security:** User data, financial education content, analytics data
- **AI and ML Security:** Training data, models, algorithms, recommendations
- **Third-Party Risk:** Vendors, service providers, integrations
- **Compliance Risk:** Regulatory requirements, contractual obligations
- **Operational Security:** Day-to-day operations, processes, procedures

2.3 Risk Treatment

2.3.1 Risk Treatment Options

- **Mitigate:** Implement controls to reduce risk
- **Transfer:** Share risk through insurance or contracts
- **Accept:** Formally accept risk when within tolerance
- **Avoid:** Eliminate risk by removing the risk source

2.3.2 Risk Acceptance Process

- Risks requiring formal acceptance: Medium and High risks
- Acceptance authority:
 - Low risk: Security Operations Manager
 - Medium risk: CISO
 - High risk: Security Steering Committee
 - Critical risk: Executive Security Committee
- Documentation requirements: Risk acceptance form with business justification, compensating controls, and review timeline

3. SECURITY POLICIES AND STANDARDS

3.1 Policy Framework

3.1.1 Policy Hierarchy

- 1. **Information Security Policy:** Overarching security direction (Board approved)
- 2. **Domain-Specific Policies:** Focused on specific security domains (Executive approved)
- 3. **Standards:** Specific requirements implementing policies (CISO approved)
- 4. **Procedures:** Step-by-step instructions (Department approved)
- 5. **Guidelines:** Recommended practices (Security team approved)

3.1.2 Key Security Policies

Policy	Purpose	Review Frequency	Owner
Information Security Policy	Overall security governance	Annual	CISO
Acceptable Use Policy	Proper use of systems	Annual	CISO
Access Control Policy	Account and access management	Annual	Security Ops Manager
Data Classification Policy	Data handling requirements	Annual	Data Security Lead
Secure Development Policy	Secure coding practices	Annual	Application Security Lead
Cloud Security Policy	AWS security requirements	Semi-annual	Cloud Security Architect
Incident Response Policy	Security incident handling	Annual	Security Ops Manager
Change Management Policy	Secure change procedures	Annual	Security Ops Manager
Vendor Security Policy	Third-party security requirements	Annual	CISO
Business Continuity Policy	Disaster recovery and continuity	Annual	CISO/COO

3.2 Standards and Procedures

3.2.1 Key Security Standards

- **Authentication Standards:** Password requirements, MFA, session management
- **Encryption Standards:** Algorithms, key management, implementation requirements
- **Network Security Standards:** Segmentation, firewall rules, remote access
- **Cloud Configuration Standards:** AWS security settings, monitoring requirements
- **Endpoint Security Standards:** Workstation/device security requirements
- **Secure Coding Standards:** Language-specific secure coding practices
- **Logging and Monitoring Standards:** Event capture, retention, alerting

3.2.2 Procedures

- Account provisioning/deprovisioning procedures
- Security incident response procedures
- Vulnerability management procedures
- Secure development lifecycle procedures
- Security assessment procedures
- Data backup and recovery procedures
- Security monitoring procedures

3.3 Policy Management

- Central policy repository with version control
- Regular review and update cycle
- Communication of policy changes
- Acknowledgement tracking
- Compliance monitoring
- Exception management process

4. SECURITY CONTROLS

4.1 Administrative Controls

4.1.1 Security Awareness and Training

- New hire security orientation
- Annual security awareness training
- Role-based security training
- Phishing simulation program
- Security newsletters and communications
- Security champions program
- Targeted training for high-risk roles

4.1.2 Personnel Security

- Background checks for all employees
- Security requirements in job descriptions
- Security responsibilities in performance reviews
- Separation procedures
- Acceptable use acknowledgement
- Non-disclosure agreements
- Disciplinary process for security violations

4.1.3 Change Management

- Security review in change process
- Pre-implementation security testing
- Rollback procedures
- Emergency change process
- Post-implementation security validation

4.2 Technical Controls

4.2.1 Identity and Access Management

- Centralized identity management
- Multi-factor authentication for all critical systems
- Role-based access control

- Principle of least privilege
- Just-in-time and just-enough access
- Privileged access management
- Regular access reviews
- Automated deprovisioning
- Strong password requirements
- Single sign-on where appropriate

4.2.2 Network Security

- Network segmentation
- Firewall protection
- Intrusion detection/prevention
- Web application firewall (WAF)
- Secure remote access (VPN)
- Network traffic monitoring
- DDoS protection
- DNS security controls
- Email security controls

4.2.3 Endpoint Security

- Endpoint protection platform
- Full disk encryption
- Mobile device management
- Patch management
- Application whitelisting
- USB/removable media controls
- Browser security controls
- Local firewall

- Host-based intrusion prevention

4.2.4 Cloud Security

- AWS security configuration following best practices
- Cloud security posture management
- Infrastructure as Code security review
- Container security
- Serverless security controls
- Cloud access security broker (CASB)
- Storage security controls
- Cloud network security
- Cloud security monitoring

4.2.5 Data Protection

- Data classification and handling
- Encryption at rest and in transit
- Database security controls
- Data loss prevention
- Data access monitoring
- Rights management
- Secure file sharing
- Data masking and anonymization
- Secure disposal procedures

4.2.6 Application Security

- Secure development lifecycle
- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Software composition analysis

- API security testing
- Penetration testing
- Security code reviews
- Input validation
- Output encoding
- Session management
- Error handling

4.2.7 AI and ML Security

- Training data protection
- Model security validation
- Adversarial testing
- AI governance controls
- Feature security review
- Output verification
- Bias detection and prevention
- AI ethics verification

4.3 Physical Controls

- Secure work environment
- Clean desk policy
- Visitor management
- Physical access control
- Environmental controls
- Physical media handling
- Secure disposal (shredding)

5. CLOUD SECURITY

5.1 AWS Security Architecture

5.1.1 AWS Account Structure

- Production account
- Development account
- Testing account
- Security and audit account
- Centralized logging account
- Cross-account access controls
- AWS Organizations implementation

5.1.2 Network Design

- VPC architecture
- Subnet segmentation
- Security groups
- Network ACLs
- Transit Gateway configuration
- VPN connectivity
- DirectConnect (if applicable)
- Load balancer security

5.1.3 Identity and Access Management

- IAM roles and policies
- Permission boundaries
- AWS SSO implementation
- Temporary credentials
- Service control policies
- Resource-based policies
- AWS CloudTrail logging

5.2 AWS Security Controls

5.2.1 Compute Security

- EC2 instance hardening
- AMI security validation
- Container security
- Lambda function security
- Auto-scaling security
- Patch management
- Host-based protection

5.2.2 Storage Security

- S3 bucket security
- EBS encryption
- RDS encryption
- DynamoDB encryption
- Backup security
- S3 access policies
- Lifecycle management

5.2.3 Monitoring and Detection

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- AWS Security Hub
- Amazon Detective
- VPC Flow Logs
- CloudWatch Alarms
- CloudWatch Events

5.2.4 Compliance and Governance

- AWS Artifact for compliance reporting
- AWS Audit Manager
- Automated compliance scanning
- Infrastructure as Code security review
- Drift detection
- Cost security controls

5.3 Cloud Security Operations

- Cloud security posture management
- Continuous monitoring
- Automated remediation
- Cloud-specific incident response
- Cloud security testing
- Cloud security metrics and reporting

6. APPLICATION SECURITY

6.1 Secure Development Lifecycle

6.1.1 Security in SDLC Phases

Planning and Requirements

- Security requirements definition
- Threat modeling
- Security user stories
- Privacy by design requirements

Design

- Security architecture review
- Database security design
- Authentication/authorization design
- API security design

Development

- Secure coding guidelines
- Security libraries and frameworks
- Code security reviews
- Secure configuration

Testing

- Unit security testing
- Integration security testing
- SAST/DAST automation
- Penetration testing

Deployment

- Secure deployment pipeline
- Infrastructure as Code security
- Production security verification
- Secure key management

Maintenance

- Security patch management
- Security debt tracking
- Security monitoring
- Vulnerability management

6.1.2 DevSecOps Integration

- Security automation in CI/CD
- Security as code
- Security testing gates
- Automated security validation
- Security metrics in pipelines

- Developer security tooling

6.2 Application Security Controls

6.2.1 Authentication and Authorization

- Modern authentication framework
- MFA for critical functions
- Role-based access control
- Fine-grained permissions
- Session management
- Account lockout/recovery
- User privilege review

6.2.2 Input Validation and Output Encoding

- Input validation strategy
- API parameter validation
- File upload security
- Output encoding
- Content security policy
- Cross-site scripting prevention
- SQL injection prevention

6.2.3 API Security

- API authentication
- API rate limiting
- Input validation
- Output validation
- Error handling
- API gateway protection
- API inventory and documentation

6.2.4 Mobile Application Security

- Mobile authentication
- Secure data storage
- Certificate pinning
- Anti-tampering controls
- Secure communication
- Mobile code obfuscation
- Secure offline operation

6.3 Security Testing

- Automated security testing
- Manual security testing
- Penetration testing (annual)
- Vulnerability scanning
- Bug bounty program (if applicable)
- Red team exercises (if applicable)
- Security regression testing

7. DATA SECURITY AND PRIVACY

7.1 Data Classification and Handling

7.1.1 Data Classification Levels

Classification Description		Examples
Confidential	Highly sensitive, strict controls	PII, authentication credentials, financial data
Restricted	Sensitive, limited access	User learning progress, aggregate usage data
Internal	For internal use, controlled access	Business documents, internal communications
Public	Approved for public release	Marketing materials, public documentation

7.1.2 Data Handling Requirements

Classification Storage		Transmission	Sharing	Disposal
Confidential	Encrypted, access-controlled	Encrypted	Authorized only, logged	Secure deletion, verification
Restricted	Encrypted, access-controlled	Encrypted	Business need, approval	Secure deletion
Internal	Standard protection	Encrypted	Internal only	Standard deletion
Public	Standard protection	Standard protection	Unrestricted	Standard deletion

7.2 Data Protection Controls

7.2.1 Data at Rest Protection

- Database encryption
- File system encryption
- Encryption key management
- Secure backup processes
- Data access logging
- Database activity monitoring
- Storage security

7.2.2 Data in Transit Protection

- TLS implementation
- Certificate management
- VPN for remote access
- API encryption
- Secure file transfer
- Email encryption
- Data validation at endpoints

7.2.3 Data in Use Protection

- Data access monitoring
- Data masking for development/testing
- Memory protection
- Secure processing environments
- Data leak prevention
- User behavior analytics
- Session protection

7.3 Privacy Controls

7.3.1 Privacy Framework

- Privacy by design principles
- Privacy impact assessments
- Data minimization practices
- Purpose limitation policies
- Consent management
- Privacy notices and policies
- Privacy training and awareness

7.3.2 Data Subject Rights Management

- Process for access requests
- Process for correction requests
- Process for deletion requests
- Process for export requests
- Rights fulfillment tracking
- Response time monitoring
- Documentation and evidence

7.3.3 Educational Data Privacy

- Student data protection

- Learning analytics privacy controls
- Parental consent processes (if applicable)
- Age-appropriate design
- Educational record protection
- Progress data privacy
- Assessment data security

8. INCIDENT MANAGEMENT

8.1 Security Incident Response Plan

8.1.1 Incident Response Team

- CISO (Incident Commander)
- Security Operations Manager
- System/Application Owners
- Technical Specialists
- Legal Counsel
- Communications Lead
- Human Resources (if applicable)
- Executive Leadership (for critical incidents)

8.1.2 Incident Response Phases

Preparation

- IR plan development and maintenance
- IR team training
- IR tools and resources
- Tabletop exercises
- Playbook development

Detection and Analysis

- Alert monitoring

- Incident classification
- Initial assessment
- Evidence collection
- Scope determination

Containment, Eradication, and Recovery

- Short-term containment
- System backup
- Long-term containment
- Threat removal
- System restoration
- Verification of security

Post-Incident Activities

- Incident documentation
- Root cause analysis
- Lessons learned
- Improvement planning
- Metrics collection

8.1.3 Incident Classification

Severity	Description	Examples	Response Time
Critical	Significant impact to business	Data breach, system compromise	Immediate (24/7)
High	Major impact to business function	Targeted attack, malware outbreak	Immediate (business hours), 2hr (off-hours)
Medium	Limited impact	Isolated security event, policy violation	Same business day

Severity Description		Examples	Response Time
Low	Minimal impact	Minor violation, informational alert	Next business day

8.2 Incident Response Procedures

8.2.1 Specialized Incident Response Procedures

- Data breach response procedure
- Malware outbreak procedure
- Account compromise procedure
- Denial of service response procedure
- Insider threat procedure
- Cloud security incident procedure
- Third-party breach procedure

8.2.2 Communication Plan

- Internal communication procedures
- External communication procedures
- Customer notification process
- Regulatory notification requirements
- Law enforcement engagement
- Incident status updates
- Post-incident communication

8.2.3 Evidence Handling

- Evidence collection procedure
- Chain of custody documentation
- Secure evidence storage
- Forensic analysis process
- Evidence preservation

- Legal hold procedure

8.3 Incident Response Testing

- Annual tabletop exercises
- Technical testing scenarios
- Red team exercises (if applicable)
- Post-exercise analysis
- Improvement implementation
- Metrics and reporting

9. VULNERABILITY MANAGEMENT

9.1 Vulnerability Management Program

9.1.1 Vulnerability Identification

- Automated vulnerability scanning
- Manual security testing
- Threat intelligence monitoring
- Bug bounty program (if applicable)
- Vendor vulnerability notifications
- Security research monitoring
- Internal vulnerability reporting

9.1.2 Vulnerability Assessment

- Vulnerability verification
- False positive identification
- Impact assessment
- Exploitability analysis
- Risk scoring methodology
- Prioritization process
- Tracking and management

9.1.3 Remediation Process

- Remediation SLAs based on severity
 - Critical: 24 hours
 - High: 7 days
 - Medium: 30 days
 - Low: 90 days
- Remediation planning
- Temporary mitigations
- Patch management
- Configuration changes
- Validation testing
- Exception process

9.2 Patch Management

- Patch identification and tracking
- Patch testing procedures
- Staged deployment approach
- Emergency patching process
- Patch verification
- Patch compliance monitoring
- Reporting and metrics

9.3 Security Debt Management

- Security debt identification
- Security debt tracking
- Prioritization framework
- Remediation planning
- Resource allocation

- Progress reporting
- Acceptance process for long-term issues

10. SECURITY MONITORING AND OPERATIONS

10.1 Security Monitoring Strategy

10.1.1 Monitoring Coverage

- Network monitoring
- Endpoint monitoring
- Cloud environment monitoring
- Application monitoring
- Database monitoring
- User activity monitoring
- Third-party access monitoring
- Physical security monitoring

10.1.2 Monitoring Approach

- Real-time monitoring
- Behavior-based analytics
- Signature-based detection
- Anomaly detection
- Correlation analytics
- Threat intelligence integration
- Automated response capabilities

10.2 Security Operations Center (SOC)

10.2.1 SOC Capabilities

- 8x5 monitoring with on-call support
- Alert triage and analysis
- Incident escalation

- Threat hunting
- Forensic investigation
- Compliance monitoring
- Reporting and metrics

10.2.2 SOC Tools

- SIEM solution
- EDR platform
- Network monitoring
- Cloud security monitoring
- Threat intelligence platform
- Ticketing system
- Digital forensics toolkit
- Automation and orchestration platform

10.3 Threat Intelligence

- Threat intelligence sources
- Intelligence analysis process
- Actionable intelligence delivery
- Intelligence integration with security tools
- Proactive threat hunting
- Intelligence sharing (if applicable)
- Effectiveness measurement

11. COMPLIANCE AND ASSURANCE

11.1 Regulatory Compliance

11.1.1 Key Compliance Requirements

Regulation/Standard	Applicability	Key Requirements	Assessment Frequency
SOC 2	Cloud Service	Security, Availability, Confidentiality, Processing Integrity	Annual
GDPR (if applicable)	EU User Data	Privacy Controls, Rights Management, DPA	Annual
CCPA/CPRA (if applicable)	CA User Data	Privacy Controls, Rights Management	Annual
FERPA (if applicable)	Educational Records	Educational Privacy, Consent	Annual
PCI DSS (if applicable)	Payment Data	Cardholder Data Protection	Annual
COPPA (if applicable)	Children's Data	Parental Consent, Protection	Annual

11.1.2 Compliance Program

- Compliance requirements mapping
- Control implementation
- Regular compliance assessments
- Gap remediation
- Documentation maintenance
- Attestation management
- Regulatory monitoring

11.2 Security Assessments

11.2.1 Internal Assessments

- Security control assessments
- Compliance self-assessments
- Security architecture reviews
- Policy compliance reviews
- Technical configuration reviews

- Risk assessments

11.2.2 External Assessments

- Independent penetration testing
- Compliance audits
- Vendor security assessments
- Red team exercises (if applicable)
- Social engineering testing
- Cloud security assessments

11.3 Reporting and Metrics

11.3.1 Executive Reporting

- Monthly security dashboard
- Quarterly security program review
- Risk posture assessment
- Key security metrics
- Improvement recommendations
- Resource requirements

11.3.2 Key Security Metrics

- Security incident metrics
- Vulnerability management metrics
- Patch compliance metrics
- Security training completion
- Control effectiveness metrics
- Access management metrics
- Third-party security metrics

12. VENDOR SECURITY MANAGEMENT

12.1 Vendor Security Assessment

12.1.1 Vendor Risk Tiering

Tier	Description	Assessment Depth	Reassessment Frequency
Tier 1	Critical data access, direct integration	Comprehensive	Annual
Tier 2	Limited sensitive data, important functions	Standard	Annual
Tier 3	No sensitive data, non-critical functions	Basic	Biennial

12.1.2 Assessment Process

- Security questionnaire
- Documentation review
- Control validation
- Compliance verification
- Vulnerability assessment
- Remediation planning
- Approval process

12.2 Vendor Contracting

- Security and privacy requirements
- Data protection obligations
- Incident notification requirements
- Right to audit clause
- Service level agreements
- Compliance attestations
- Subcontractor management
- Termination provisions

12.3 Ongoing Vendor Management

- Performance monitoring
- Compliance verification

- Security incident management
- Service level monitoring
- Annual reassessment
- Vulnerability notification process
- Contract renewal review
- Offboarding process

13. SECURITY AWARENESS AND TRAINING

13.1 Security Awareness Program

13.1.1 Program Components

- New hire security orientation
- Annual security awareness training
- Monthly security newsletters
- Security alerts and advisories
- Awareness campaigns
- Phishing simulations
- Security reminders and tips
- Security portal and resources

13.1.2 Key Awareness Topics

- Phishing and social engineering
- Password and authentication
- Data protection and handling
- Clean desk and physical security
- Mobile device security
- Remote work security
- Social media security
- Incident reporting

13.2 Specialized Security Training

13.2.1 Role-Based Training

Role	Training Focus	Frequency
Developers	Secure coding, OWASP Top 10, secure design	Annual
IT Operations	Secure configuration, patch management, monitoring	Annual
Data Scientists	AI/ML security, data protection, model security	Annual
Content Creators	Content security, intellectual property protection	Annual
Executives	Security leadership, risk management, incident response	Annual

13.2.2 Security Certification Support

- Industry certification identification
- Training resources
- Certification support
- Continuous education

13.3 Measuring Effectiveness

- Training completion rates
- Phishing simulation metrics
- Security incident trends
- Security behavior assessments
- Knowledge assessments
- Feedback collection
- Program improvement

14. BUSINESS CONTINUITY AND DISASTER RECOVERY

14.1 Security Aspects of Business Continuity

- Security requirements for business continuity
- Security in disaster scenarios

- Alternative processing security
- Crisis authentication procedures
- Emergency access protocols
- Security monitoring during recovery
- Data protection during recovery

14.2 Backup and Recovery Security

- Backup encryption
- Backup access controls
- Backup testing security
- Secure off-site storage
- Recovery validation
- Restoration testing
- Backup system security

14.3 Disaster Recovery Testing

- Security in DR tests
- Security validation after recovery
- Secure communication during DR
- Access control testing
- Data integrity verification
- Security monitoring during recovery
- Security lessons learned

15. PROGRAM MAINTENANCE AND IMPROVEMENT

15.1 Security Program Assessment

- Annual program effectiveness assessment
- Maturity model assessment
- Gap analysis

- Benchmark comparison
- Control effectiveness testing
- Resource adequacy evaluation
- Program improvement planning

15.2 Continuous Improvement

- Lessons learned process
- Control enhancement program
- Security architecture evolution
- Technology refresh planning
- Efficiency improvement initiatives
- Automation opportunities
- Resource optimization

15.3 Security Roadmap

15.3.1 Short-term Initiatives (0-6 months)

- Complete security policy updates
- Enhance AWS security monitoring
- Implement vulnerability management improvements
- Enhance identity management controls
- Develop specialized security training

15.3.2 Medium-term Initiatives (6-18 months)

- Enhance application security program
- Implement advanced data protection
- Improve security automation
- Enhance third-party risk management
- Develop security metrics program

15.3.3 Long-term Initiatives (18-36 months)

- Security architecture modernization
- Advanced security analytics
- Comprehensive security automation
- Enhanced threat intelligence capabilities
- Security program optimization

APPENDICES

Appendix A: Security Policy List

1. Information Security Policy
2. Acceptable Use Policy
3. Access Control Policy
4. Data Classification and Handling Policy
5. Secure Development Policy
6. Cloud Security Policy
7. Incident Response Policy
8. Vulnerability Management Policy
9. Password Policy
10. Remote Access Policy
11. Mobile Device Policy
12. Encryption Policy
13. Security Monitoring Policy
14. Physical Security Policy
15. Vendor Security Management Policy
16. Security Awareness Policy
17. Business Continuity Policy
18. Asset Management Policy
19. Network Security Policy

20. Change Management Policy

Appendix B: Security Incident Response Plan

Incident Response Team Contact Information

- CISO: [Name, Contact Details]
- Security Operations Manager: [Name, Contact Details]
- IT Operations Lead: [Name, Contact Details]
- Application Security Lead: [Name, Contact Details]
- Legal Counsel: [Name, Contact Details]
- Communications Lead: [Name, Contact Details]
- Executive Escalation: [Name, Contact Details]

Incident Classification Matrix

- Details on severity levels and response requirements

Incident Response Procedures

- Step-by-step response procedures
- Communication templates
- Evidence handling guidelines
- Reporting requirements

Post-Incident Analysis Template

- Incident timeline
- Root cause analysis
- Impact assessment
- Remediation effectiveness
- Lessons learned
- Improvement recommendations

Appendix C: Security Awareness Materials

- Sample security awareness content

- Phishing simulation examples
- Security communication templates
- Training evaluation forms
- Role-based training outlines

Appendix D: Risk Assessment Templates

- Risk assessment methodology
- Risk register template
- Risk treatment plan template
- Risk acceptance form
- Control effectiveness assessment

Appendix E: Security Implementation Roadmap

Phase 1: Foundation (Months 1-3)

- Establish security governance structure
- Develop/update key security policies
- Implement basic security monitoring
- Establish incident response capability
- Launch security awareness program

Phase 2: Enhancement (Months 4-9)

- Enhance cloud security controls
- Implement vulnerability management program
- Develop application security program
- Enhance data protection controls
- Implement vendor security program

Phase 3: Optimization (Months 10-18)

- Enhance security automation
- Improve security metrics and reporting

- Develop advanced monitoring capabilities
- Enhance security integration
- Optimize security operations

Phase 4: Maturation (Months 19-24)

- Advanced threat detection capabilities
- Comprehensive security integration
- Enhanced security analytics
- Mature risk management program
- Continuous improvement framework






Stickball_ManSAU37_NH_14State_OHG_vendorsigned_securityattach

Final Audit Report

2025-06-23

Created:	2025-06-23
By:	Deborah Lutz (dlutz@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAGAWMVWcSyXYM-mDHfU7HpF7AiMBtum36

"Stickball_ManSAU37_NH_14State_OHG_vendorsigned_securityattach" History

-  Document created by Deborah Lutz (dlutz@tec-coop.org)
2025-06-23 - 1:48:59 PM GMT
-  Document emailed to STEVE CROSS (scross@mansd.org) for signature
2025-06-23 - 1:49:10 PM GMT
-  Email viewed by STEVE CROSS (scross@mansd.org)
2025-06-23 - 2:02:05 PM GMT
-  Document e-signed by STEVE CROSS (scross@mansd.org)
Signature Date: 2025-06-23 - 2:03:46 PM GMT - Time Source: server
-  Agreement completed.
2025-06-23 - 2:03:46 PM GMT