SOUTH SAN ANTONIO INDEPENDENT SCHOOL DISTRICT

Agenda Item Summary

Meeting Date: December 15, 2025

Agenda Section: Discussion and Possible Action

Agenda Item Title: Teach for America Partnership and Service Agreements

From/Presenters: Rita Uresti, Executive Director of Human Resources

Description: The District proposes to enter into a partnership with Teach For America (TFA) San Antonio to enhance teacher recruitment and expand tutoring interventions by adding 25 new TFA corps members to serve as certified classroom teachers. In addition, the Teach For America–Ignite program will provide trained Fellows who will deliver targeted small-group virtual tutoring to support student learning.

Teach For America is a nationally recognized organization that recruits, trains, and supports educators who are committed to advancing student success in under-resourced districts. Under this agreement, TFA will supply qualified teachers and Ignite tutors, while the District provides placement, mentorship, and ongoing support to ensure alignment with our instructional goals and staff development efforts.

Since 2010, TFA San Antonio has placed over 750 teachers in local schools and built a strong alumni network that continues to support student success and serve in leadership roles across the community.

Historical Data: This will be the first formal agreement with Teach For America San Antonio.

Recommendation: Approve the Teach For America Partnership and Service Agreements.

Purchasing Director and Approval Date: Not applicable

Funding Budget Code and Amount: Not Applicable

Goal: 2. SSAISD will recruit, develop, support, and retain effective teachers, principals, and other instructional staff.

Teach For America

SOUTH SAN ANTONIO ISD

BOARD MEETING

DECEMBER 15, 2025

Overview

1. Mission and Vision
2. Services Provided
3. Partnering with TFA

Our Vision

One day, all children will have the opportunity to attain an excellent education.

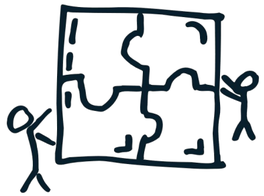
Our Mission

Teach For America finds, develops, and supports extraordinary leaders to transform education and expand opportunity for all students.

Our 2030 Goal

By 2030, twice as many children in communities where we work will be college and career ready, indicating that they are on a path to economic mobility and co-creating a future filled with possibility.

How TFA is Taking Action



Find and Develop Talent

We recruit, train, and support new educators, who we call corps members.

Ensure Student Success

We set up feedback processes and learning to ensure student success.

Advance Systems Change

We develop the long-term leadership of our members and partner with others across the region.

Recruitment

- We recruit extraordinary, action-oriented leaders, from all backgrounds, early in their careers.
- Four national, state, and local recruitment campaigns over the course of the year
- Provide financial assistance to bridge the transition to teaching
    - $3,500-$6,500 depending on need

Pre-Service Training

- Partner with Southern Methodist University and ACT-RGV's certification programs to ensure teachers are eligible to teach on an intern certificate
- Conduct hybrid training May-July focused on instruction, classroom environment, and reflective practices
- Teach summer school under the supervision of a certified mentor teacher
- Ensure a day-one ready teacher

In-Service Training

- During two-year corps program, all teachers are assigned a Teach For America coach to co-create an individualized learning plan
- Access to a multitude of digital resources, including on-demand coaching via Better Lesson, high quality resources, differentiated trainings, and wellness supports
- Reflective conversations on developing passion and skills over the course of

Alumni Support

- After our initial two year program, our members become alumni
  - 500 alumni in San Antonio
- Alumni have access to a career center to access additional resources and training
- Locally, across Texas, and nationally we provide optional training and fellowships targeting school leadership and other key leadership roles in education.

Partnership Services

Recruit and Train New Teachers

Districts with a signed contract have access to interview and hire TFA candidates.

Districts and TFA align on the process for navigating district hiring systems.

Support New Teachers

Additional assigned coach for any teacher in their first and second year.

On-demand digital resources which can be customized based on teacher need.

Access to wellness and other resources to meet the

Monitor Student Success

Collaborate on data sharing to support teacher development and track student success (data sharing agreement).

Collaborate with district personnel to accelerate the teacher development leading to student success.

Build Lifelong Leaders

Support alumni who remain in education through leadership development opportunities and university partnerships.

Collaborate with partner districts to develop talent pipelines for campus and district leadership roles.

Our Partnership Agreement

- 5-year agreement for corps member placements.
- $5,000 annual fee per corps member for recruitment, certification, and training.
- District hires and places up to 25 corps members in high-needs vacancies.
- TFA provides training, coaching, and performance monitoring throughout the two-year corps commitment.

Partnering for Student Success

Teach For America

MASTER PROFESSIONAL SERVICES AGREEMENT

This master professional services agreement (this "Agreement") is dated December 15, 2025 and is entered into between TEACH FOR AMERICA, INC. ("Teach For America" or "TFA"), a Connecticut non-profit with regional office located at 1209 South Saint Mary's Street, San Antonio, TX 78210 and South San Antonio Independent School District, a political subdivision of the state of Texas ("School Partner") located at 5622 Ray Ellison Blvd, San Antonio, TX 78242 (each individually "a Party" and collectively "the Parties").

RECITALS

WHEREAS, Teach For America is a national leader in recruiting, selecting, training and providing ongoing professional development to individuals committed to closing the achievement gap by serving as effective classroom teachers during their two-year service commitment specifically equipped to enhance student achievement in under-resourced school systems ("Corps Members" or "Teachers"). Upon successful completion of their two-year service commitment, said Corps Members become alumni of Teach For America ("Alumni"). (Corps Members and Alumni are collectively known as "Participants").

WHEREAS, Teach For America established various Fellowships ("Fellowships") aimed at helping selected individuals, such as Teach For America's Participants strengthen their leadership in Teach For America's partner schools.

WHEREAS, Teach For America agrees to provide the professional services identified in each Statement of Work (as hereinafter defined) to perform the services (the "Services") identified in each Statement of Work and School Partner would like to receive such Services and agrees to compensate Teach For America as set forth and subject to the terms and conditions set forth below;

NOW THEREFORE, School Partner and Teach For America agree to be bound by the terms and conditions of this Agreement.

AGREEMENT

I. THE SERVICES:

A. *The Services: Statements of Work*. Teach For America will provide the Services described in each written work statement (each, a "Statement of Work" or "SOW"), by agreement of the parties, for the fees and in accordance with the timeframe, if any, set

forth therein. A SOW will set forth requirements for a specific project, or may set forth a general description of the type of services that Teach For America will provide to the School Partner. In the event of any conflict between the Standard Terms and Conditions of this Agreement and the Special Terms and Conditions of a SOW, the Special Terms and Conditions of the SOW shall control for purposes of the Services performed under that specific SOW only.

II. COMPENSATION:

A. *Fees*. The School Partner will pay Teach For America as compensation for the Services the fees described in each SOW in accordance with the terms set forth in such SOW and as substantiated by invoices provided by Teach For America.

B. *Invoices; Disputed Amounts*. Unless otherwise specified in the applicable SOW, Teach For America will deliver a written invoice to School Partner on an annual basis setting forth the fees payable by School Partner in respect to the current year's work. Teach for America and the School Partner agree that Teach for America will invoice for each school year no earlier than November 30th of that current school year. The Parties agree that if a Teach for America Corps Member is not a good fit for the School Partner, the School Partner may decide to terminate the Corps Member in accordance with applicable law, regulation, and District policy; in such event, if the District notifies Teach for America of the termination of a particular Corps Member on or before November 15th of the current school year, Teach for America will waive the annual fee for that particular Corps Member. Within thirty (30) days of receipt of an invoice, School Partner will either pay the same (in whole or in non-disputed part) or will notify Teach For America that some or all of the fees set forth therein are in dispute. The parties will promptly work to resolve any such disputes and upon resolution if any agreed-upon amounts are due and payable, School Partner will promptly pay Teach For America the agreed-upon amounts (if any).

C. *Non-refund*. Teach For America shall have no obligation to refund to School Partner any amount paid by School Partner in respect of any Service under any SOW for any reason whatsoever unless the amount was an overpayment.

D. *Withholding*. Teach For America is responsible for payment of all taxes incurred in connection with performance of the Services by Teach For America.

III. TERM AND TERMINATION:

A. *Term*. The Term of this Agreement will commence on the Effective Date and will remain in effect for five years. Specifically, this Agreement will expire on September 25, 2030 but all provisions related to SOWs created during this time period will remain in effect through the conclusion of said SOWs unless earlier terminated pursuant to Sections B.ii below.

B. *Termination*.

i. The Parties may terminate this Agreement at any time by mutual written consent.

ii. Either Party may terminate:

(a.) This Agreement at any time, without any prior notice in the event that the other Party is unable to fulfill its obligations pursuant to this Agreement, except that if School Partner is unable to fulfill its obligations, School Partner shall have the right to exercise its opportunity to cure; such opportunity to cure the inability to fulfill its obligations will extend up to thirty (30) business days and may be further extended upon mutual agreement of the parties. The Parties understand and agree that Teach For America may not be able to perform or provide the services until the School Partner fulfills its obligations. Such inability to perform/provide the services during this period shall in no way be seen as a default on the part of Teach For America. Upon any such termination, TFA shall be paid for all work completed up through the date of termination unless otherwise prohibited by law. Any early termination of this Agreement subject to this section will result in the automatic termination of all SOWs connected herewith.

(b.) This Agreement upon written notice, if the other Party is in breach of any of its material obligations, representations or warranties hereunder, and does not cure such breach within ten (10) business days of receipt of a written demand for cure. Any termination of this Agreement will result in the automatic termination of all SOWs connected herewith. Upon any such termination, Teach For America shall be paid for all work completed under the corresponding SOWs up through the date of termination unless otherwise prohibited by law.

(c.) any individual SOW, with or without cause, upon ninety (90) business days prior written notice. Upon any such termination, TFA shall be paid for all work completed under the corresponding SOW up through the date of termination unless otherwise prohibited by law.

IV. STANDARD TERMS AND CONDITIONS

A. *Ownership of Intellectual Property*. For purposes of this Agreement, "*Work Product*" means, collectively, all work product created, conceived, developed or first reduced to practice by TFA pursuant to this Agreement. TFA will own all right, title and interest in all Work Product, including without limitation all subject matter for which TFA may obtain and hold copyrights, patents, registrations, and any intellectual property or other protections that may be available to TFA.

B. *Confidentiality*. Each Party shall hold all non-public information, written or oral, whether or not it is marked as confidential, that the Disclosing Party disclosed or made available to the Receiving Party, directly or

indirectly, through any means of communication (the "Confidential Information") in confidence in accordance with the terms of this Agreement. Confidential Information shall only be used in accordance with the terms of this Agreement and the Receiving Party shall exercise at least the same degree of care as it uses with its own confidential information, but in no event less than reasonable care. The Receiving Party may disclose Confidential Information to 1) its representatives but only to the extent necessary to carry out the terms of this Agreement and 2) to a third-party only if required to do so, and only to the extent required, by law. All additional provisions related to data sharing between the Parties, if any, will be outlined in a separate data sharing agreement SOW, and are incorporated herein by reference.

C. *FERPA and Data Privacy*.

i. School Partner may disclose to Teach For America student-related records and personally identifiable information contained in such records (collectively, "Student Records") in the course of providing the professional development and data storage services outlined in individual SOWs . Pursuant to its obligations under the Family Educational Rights and Privacy Act, 20 USC §1232g, and its implementing regulations, 34 CFR pt. 99 and §99.31(a)(1) , as each may be amended from time to time ("FERPA"), while providing the services, Teach For America is a school official with legitimate educational interests in the Student Records.

ii. Teach For America agrees to use, maintain, and disclose Student Records strictly in accordance with the requirements of FERPA, as permitted by any SOW and/or otherwise authorized by the School Partner or by law, and in compliance with student data privacy requirements contained any potential separate data sharing agreement SOW, and only for the purposes for which disclosure was made. While the Parties understand and agree that it unequivocally remains the School Partner's obligation to monitor changes in federal, state and local law as it pertains to student data to ensure School Partner's compliance, Teach For America will notify the School Partner prior to processing Student Records if Teach For America discovers a conflict between the requirements of FERPA, the authorizations in the SOW and/or other authorizations provided by the School Partner.

iii. Teach For America may re-disclose Student Records to third party service providers to the extent required to provide the Teach for America services pursuant to Teach For America's provision of the professional development and data storage services outlined in any SOW, as provided in 34 C.F.R. § 99.33(b), provided that Teach For America shall, in advance, provide the names of such parties and a brief description of such parties' legitimate educational interest in receiving such information. Except as strictly required to provide the services to School Partner, Teach for America will not sale, transfer, barter, or otherwise make available the Student Records or confidential School Party information to any third party. Teach for America shall

implement contractual obligations with is third-party service providers that require its third-party service providers to maintain the confidentiality and security of Student Records.

iv. Pursuant to 34 CFR § 99.7(a)(3)(iii), School Partner shall include, in its annual notification of rights under FERPA, criteria that qualify Teach For America, in its capacity as a provider of professional development and data storage services, as a school official with a legitimate educational interest.

D. [intentionally omitted]

E. *Participant Suitability and Responsibilities.*

i. Teach For America's Obligations. Teach for America shall conduct background checks, including criminal background checks as permitted by applicable law, and provide interviews for all Participants recommended to School Partner. TFA shall ensure that Participants hold the required licensures and qualifications required by law to perform the Services, in accordance with applicable laws, regulations, and industry standards. Teach For America shall promptly notify School Partner if it becomes aware that any Participant becomes ineligible via information revealed in background checks or loss of licensures, credentials or qualifications.

ii. School Partner's Hiring Authority. School Partner retains sole discretion and responsibility for all hiring decisions regarding all Participants. School Partner shall review all background check results and interview materials provided by Teach For America and make its own independent determination regarding the suitability and fitness of any Participant for the specific role and School Partner's environment. School Partner may, in its sole discretion, decline to hire or request reassignment of any Participant at any time.

iii. Limitations of Warranties: While Teach For America conducts reasonable screening as described above, Teach For America's screening and recommendations do not constitute a guarantee of performance or suitability for School Partner's specific needs.

iv. Responsibility for Acts and Omissions: Once hired by School Partner for purposes of their service delivery. School Partner assumes responsibility for supervision and oversight of Participants. Teach For America shall not be liable for any acts or omissions of Participants in their capacity as School Partner's employees, except to the extent such issues arise from Teach For America's material breach of its screening obligations set forth above or to the extent such acts or omissions occur during Teach for America training sessions, voluntary Teach for America events, or Teach for America off-sites.

F. *No Employment Relationship with Participants, Fellows or Facilitators.* This agreement does not permit Teach For America to function as a representative of any Participant, Fellow or Facilitator nor for Participants, Fellows or Facilitators to function as agents of Teach For America. Nothing in this Agreement shall be construed to

imply that an employer-employee relationship exists between Teach For America, Participants, Fellows or Facilitators nor permit Teach For America to interfere with any potential employment agreement or relationship between the School Partner, Participants, Fellows or Facilitators.

G. *Data Sharing*. The Parties hereby enter into the Data Sharing Agreement attached hereto as Exhibit 1 and incorporated into this Agreement by reference in its entirety.

H. *Security Measures*. Teach For America will comply with its information security policy set forth as Exhibit 2.

I. *Dismissal of Participants, Fellows and Facilitators.* Teach For America, in its sole discretion, may dismiss any such individual, with or without notice, from any program outlined on any associated SOW, for any reason whatsoever. Teach for America acknowledges and understands that School Partner, in its sole discretion, may dismiss any such individual, with or without notice to Teach for America, from any program outlined on any associated SOW.

J. *Mutual Indemnification*. To the extent permitted by law, each Party shall indemnify and hold harmless the other party and its officers, directors, employees and agents (the "Indemnitees") from and against any and all losses, liabilities, claims, damages, costs and expenses (including attorneys' fees) ("Losses") to which such Indemnitee may become subject arising out of a breach of this Agreement by the indemnifying party, except to the extent such Losses result from the willful misconduct or negligence of such Indemnitee.

K. *Insurance.* During the term of this Master Services Agreement, each Party shall maintain in force adequate workers' compensation, commercial general liability, errors and omissions, employment, and other forms of insurance, with policy limits sufficient to protect their interests and indemnify the other Party and its affiliates, and each of their officers, directors, agents, employees, subsidiaries, partners, members, controlling persons, and successors and assigns, from any losses resulting from the indemnifying Party's conduct, acts, or omissions of their agents, contractors or employees.

L. *Copyright and Trademark.* Neither Party may use the logo, name or other identifying marks of the other Party in any written materials, including materials available in an online format, without the express written permission of the other Party.

M. *Non-Publicity.* Teach for America agrees that it will not, without the prior written consent of School Partner, use the name, logo, or any identifying marks of School Partner, its trustees, agents, personnel, representatives, or students in any form of publicity, advertising, or public announcement. This includes, but is not limited to, press releases, social media posts, news articles, website content, and promotional materials. Teach for America will not publicly endorse nor disparage School Partner or its programs.

N. *Compliance with Anti-Harassment and Non-Discrimination Regulations*. By entering into this Agreement,

both Parties warrant compliance with local, state and federal anti-harassment and non-discrimination laws and regulations. The parties acknowledges that the other's violation of these laws and regulations are a breach of contract. School Partner will harassment policies and/or procedures are available at https://pol.tasb.org/PolicyOnline?key=177 and Teach for America is responsible for accessing and reviewing those policies prior to signing this MSA.

O. *Survival*. Upon termination of this Agreement all obligations hereunder shall terminate except for the obligations set forth in Sections related to *Ownership of Intellectual Property; Confidentiality; FERPA and Data Privacy; Participant Suitability and Responsibilities; No Employment Relationship with Participants, Fellows and Facilitators; Mutual Indemnification; Copyright and Trademark; and Exhibit 1,* all of which will survive any termination hereof for any reason.

P. *Notices*. Any notices to either Party under this Agreement shall be in writing and delivered by hand or sent by nationally recognized messenger service, or by registered or certified mail, return receipt requested, to the addresses set forth below or to such other address as that Party may hereafter designate by notice.

SOUTH SAN ISD
NAME:
TITLE:
ADDRESS:
EMAIL:

TEACH FOR AMERICA
TITLE:
NAME:
ADDRESS:
EMAIL:

WITH AN ELECTRONIC COPY TO: LegalAffairs@teachforamerica.org
*send only notices related to breach of contract and indemnity

Q. *Severability*. If any term or provision of this Agreement is determined to be illegal, unenforceable or invalid in whole or in part for any reason, such provisions or part thereof shall be stricken from this Agreement, and such provision shall not affect the legality, enforceability or validity of the remainder of this Agreement. Such stricken provision shall be replaced, to the extent possible, with a legal, enforceable and valid provision that is as similar in tenor to the stricken provision as is legally possible.

R. *Waiver*. A waiver or a breach or default under this Agreement shall not be a waiver of any other subsequent breach or default. The failure or delay in enforcing compliance with any term or condition of this Agreement

shall not constitute a waiver unless expressly waived in writing .

S. *Amendment/Modification/Extension*. Any amendment, modification, extension must be in writing and signed by each Party.

T. *Non-Assignment*. Neither this Agreement nor any of the rights, interests or obligations under this Agreement shall be assigned, in whole or in part, by operation of law or otherwise by either Party without the prior written consent of the other Party.

U. *Governing Law*. This Agreement and all matters relating hereto shall be governed by, construed and interpreted in accordance with the laws of the State of Texas. The Parties agree that any legal action or proceeding arising out of or relating to this Agreement shall be brought exclusively in Bexar County, Texas.

V. *Entire Agreement; Headings; Execution*. This Agreement (including all SOWs and Exhibits) sets forth the entire understanding of the parties with respect to its subject matter and supersedes any and all prior agreements, arrangements and understandings relating to the subject matter hereof. Headings are for convenience only and are not to be used to interpret this Agreement. This Agreement may be executed in separate counterparts, and all such counterparts will constitute one and the same instrument.

[MASTER PROFESSIONAL SERVICES SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, each of School Partner and Teach For America has caused its duly authorized representative to sign this Master Professional Services Agreement in the space provided below.

South San Antonio Independent School District		Teach For America	
By:		By:	
Name:	Dr. Saul Hinojosa	Name:	Nick Garcia
Address:	5622 Ray Ellison Blvd San Antonio, TX 78242	Title:	Executive Director
		Address:	1209 S. St. Mary's St. San Antonio, TX 78210

Teach For America

Contract Owner Attestation:

This contract required legal changes to the required terms and was reviewed/approved by TFA Legal Affairs in this final form.

This contract did not require legal changes and was not reviewed by TFA Legal Affairs.

Name: Verónica Díaz

Title: Senior Managing Director, Network Impact

SOW #1 Corps Member Placement Services Agreement
to the Teach For America Master Professional Services Agreement

RECITALS

This Statement of Work #1 (hereinafter called the "SOW") is issued pursuant to the Master Professional Services Agreement between Teach For America, Inc. (also described as "TFA") and South San Antonio ISD] ("School Partner"), effective December 15, 2025 (the "MSA"). This SOW is subject to the Standard Terms and Conditions contained in the MSA and the Special Terms and Conditions contained within this SOW and is made a part thereof. Any term not otherwise defined herein shall have the meaning specified in the MSA. In the event of any conflict or inconsistency between the terms of this SOW and the terms of the MSA, the terms of this SOW shall govern and prevail for the purposes of this SOW only.

The Exhibit(s) to this SOW, if any, shall be deemed to be a part hereof. In the event of any inconsistencies between the terms of the body of this SOW and the terms of the Exhibit(s) hereto, the terms of the body of this SOW shall prevail.

Accordingly, School Partner and Teach For America agree to be bound by the terms and conditions of this SOW.

SOW #1 AGREEMENT

I. CORPS MEMBER CANDIDATE RECRUITMENT, SELECTION AND HIRING: School Partner Responsibilities

A. *Consideration for Hire.*

i. Teach For America will use its reasonable commercial efforts to provide multiple teacher candidates for consideration for employment with School Partner ("Corps Members") each academic year that meet the range of grades and subject matters requested by school ("Candidate Details") as identified in **Schedule A, Chart A**. While School Partner acknowledges Teach For America may not be able to provide the referenced number of candidates and agrees to consider every candidate for employment, School Partner shall only pay the fee for each Teacher hired under this Agreement as set forth in section V herein.

ii. School Partner shall collaborate with Teach For America in good faith to identify individual schools within School Partner appropriate for Corps Members, as identified on **Schedule A, Chart B,** below. School Partner shall also consider for hire each Teacher provided by Teach For America who meets the School Partner's eligibility requirements.

iii. Any Corps Member hired by the School Partner shall be hired as the classroom teacher of record and not for substitute, auxiliary, resource or teacher's aide positions; hired for vacancies across the full range of grades and subject matters; and not restricted or limited to so-called "critical" or "shortage" subjects or grade level vacancies. School Partner agrees that it will not place Teach For America Corps Members at any for-profit schools within its district. .

B. *Hiring Process.*

i. School Partner and Teach For America will collaborate in good faith to facilitate the efficient hiring of individual Corps Members, in accordance with the School Partner's established District hiring practices

ii. School Partner shall participate in TFA hiring procedures during spring semester and submit employment offers to Corps Members no later than August 1st of the proceeding academic school year. School Partner agrees that where possible, Teach For America shall be informed of individual Corps Member's grade and subject level assignments prior to the start of their Pre-Service Training (as defined below).

iii. Subject to its obligations under pre-existing collective bargaining agreements, contracts, or applicable law, School Partner will consider offering alternative employment to any Corps Member who is not employed by the first day of the academic school year. "Alternative employment" includes, but is not limited to substitute teaching positions, "pool" teaching positions, classroom aides or other temporary category of employment available within School to individuals with teaching credentials.

II. CORPS MEMBER CANDIDATE RECRUITMENT, SELECTION AND HIRING: Teach For America Responsibilities

A. *Candidate Recruitment and Selection*. Teach For America will recruit, select for participation in the Teach For America program, and present to the School Partner for employment Corps Members from a broad range of academic majors, career fields and diverse backgrounds. Teach For America will not knowingly engage in any unlawful acts of discrimination in its recruiting or selection of candidates.

B. *Pre-Service Training and Certification Status*. Prior to entering the classroom, Teach For America will ensure each Teacher participates in pre-service training ("Pre-Service Training"). There is no cost to the District for the Teach for America pre-service training. Teacher participants will be attending as volunteers of Teach For America and not as part of their employment contract with the District. Pre-Service Training ensures that such Corps Members meet applicable federal, state and/or local educational standards or requirements such as those set forth in the federal Every Student Succeeds Act and other

applicable state certification regulations (together, the "Requirements"). For purposes of this Section and unless otherwise required by law, only those Requirements in effect at the time that the Teacher is offered employment by School Partner will be applicable.

III. CORPS MEMBER PLACEMENT AND PROFESSIONAL DEVELOPMENT COMMITMENTS: School Partner Responsibilities

A. *Employment Status.*

i. Every Corps Member employed by School Partner under this SOW shall be a full-time employee of School Partner with all the rights, including those related to compensation and benefits, responsibilities and legal protections as are provided to other teachers employed by School Partner who are similarly situated in terms of credentialing, certification and tenure status. Nothing in this SOW shall be construed to grant additional employment rights to individual Corps Members.

ii. School Partner may continue to employ individual Corps Members beyond the two-year commitment by mutual agreement between School Partner and such Corps Member. Employment beyond the two-year commitment will not require School Partner to incur or pay any additional fees to Teach for America in connection with that Corps Member.

B. *Reductions in Force*. Subject to any obligations under pre-existing labor agreements and applicable municipal and state laws and regulations, School Partner will comply with applicable law, regulations, and District Policy in its treatment of any Corps Member employed in connection with this SOW, including regarding reductions in force, eliminations, and terminations and will not discriminate against any Corps Member on the basis of their participation as a Teach for America Corps Member.

C. *Prohibited Activities and AmeriCorps Service Requirements*. School Partner acknowledges that Corps Members serving at schools may be serving as members of AmeriCorps, and as such, are subject to the rules and requirements of AmeriCorps and the Serve America Act and are required to refrain from engaging, directly or indirectly in certain activities while teaching, accumulating service hours towards an education award or otherwise engaging in activities supported by the AmeriCorps program (45 CFR § 2520.65). These restrictions pertain to when Corps Members are enrolled in the AmeriCorps program and are on the clock at their school, including teaching time, passing and planning periods and professional development sessions. School Partner will not require Corps Members to engage in any Prohibited Activities and shall post a list of Prohibited Activities in all locations where Corps Members

serve and shall complete the AmeriCorps Service Verification form as needed.

Schedule B but in general, Corps Members may not (1) provide religious instruction, (2) attempt to influence legislation or (3) participate in or endorse political events or activities. For the avoidance of doubt, Corps Members may exercise their rights as private citizens and may participate in the activities listed above on their initiative, on non-AmeriCorps time, and using non- CNCS (Corporation for National and Community Service) funds.

IV. CORPS MEMBER PLACEMENT AND PROFESSIONAL DEVELOPMENT COMMITMENTS:

Teach For America Responsibilities

A. *Professional Development and On-Line Data Storage Services*.

i. Teach For America shall provide professional development services and activities for participating Corps Members as well as on-line data storage services during the Corps Members first two years in the classroom (the "Professional Development Services"). If professional development services must be provided virtually, at Teach For America's discretion, Teach For America shall provide equivalent services to the extent possible. To facilitate provision of these professional development services, Teach For America may provide on-line data storage services, including transfer and storage of identifiable student information on Teach For America's software and servers ("Data Storage Services").

ii. While providing the Professional Development and Data Storage Services, Teach For America shall comply with the requirements of FERPA, reasonable industry standards for information security and data protection, confidentiality and cybersecurity as outlined in the original Master Services Agreement, and in compliance with requirements contained in any separate data sharing SOW.

B. *Certification and Credentialing Services.*

i. Where required, Teach For America shall facilitate the enrollment of individual Corps Members in an alternative certification/licensure program that will enable the individual Teacher to obtain appropriate credentials to be a classroom teacher of record according to the requirements of the Every Student Succeed Act and applicable state regulations in existence at the time of signature of this SOW.

ii. Teach For America shall not be responsible for and shall not be in breach of any provision of this SOW, in the event of any failure by an individual Teacher to fulfill their obligations to maintain their teaching credentials or obtain necessary waiver(s) to remain a classroom teacher of record.

V. SPECIAL TERMS AND CONDITIONS OF SOW #1

A. *Fees-for-Service*.

i. School Partner shall pay Teach For America an annual fee for each Corps Member employed under this SOW. All payments for fees shall be in the form of check delivered to Teach For America or wire transfer to an account designated by Teach For America in writing.

ii. With respect to each Corps Member whose employment by School Partner is to commence in the 2026-2027 academic year, School Partner shall pay Teach For America an annual amount of $5,000 for each year in which such Corps Member is employed by School Partner, up to two years from the date such employment is to commence. Teach for America will invoice School Partner for each current school year no earlier than November 30th of each school year. If the District decides to terminate a Corps Member, Teach for America will waive the $5,000 yearly fee for that particular Corp Member(s) so long as School Partner notifies Teach for America of the termination by November 15th of that school year.

B. *Invoicing and Payment*. Teach For America will invoice School Partner for all amounts due with respect to any academic year within thirty (30) days of the start of the academic school year, provided that Teach For America's failure to do so, will not constitute a waiver of any of Teach For America's rights or constitute a breach by Teach For America.

C. *Term*. The term of this SOW will cover all Corps Members whose employment begins with the School Partner during the 2026 – 2027 school year and continue through the school years 2027-2028, 2028-2029, 2029-2030, 2030-2031. This SOW will expire on the last school day of the 2031-2032 academic year.

D. *Termination*. This SOW may be terminated as follows:

i. at any time by mutual written agreement of the Parties;

ii. by either Party, upon thirty (30) days' prior written notice to the other Party,

iii. by either Party upon written notice to the other Party in the event of a material breach of this SOW or the underlying MSA that is incapable of being cured or, if capable of being cured, is not cured within thirty (30) days following receipt by the breaching Party of written notice of such breach from the non-breaching Party.

E. *Survivability and Effect of Termination of this SOW*. In the event of the expiration or termination of this SOW, this SOW shall become void, with the exceptions that Section IIIE (Prohibited Activities and AmeriCorps Service Requirements) shall survive and will remain in effect until such time as there are no Corps Members employed under this contract. Additionally, Teach For America will be entitled to all

outstanding amounts due up to the date of expiration or termination. Terminating this individual SOW does not terminate the MSA.

F. ***Authority***. This Agreement supersedes all communications between the parties related to the subject matter of this SOW.

SOW #1 - ACCEPTANCE FOLLOWS

IN WITNESS WHEREOF, each of School Partner and Teach For America has caused its duly authorized representative to sign this Statement of Work #1 re Corps Member Placement Services in the space provided below.

South San Antonio Independent School District		Teach For America	
By:		By:	
Name:	Dr. Saul Hinojosa	Name:	Nick Garcia
Address:	1450 Gillette Blvd	Title:	Executive Director
	San Antonio, TX 78224		
		Address:	1209 S. St. Mary's St.
			San Antonio, TX 78210

SCHEDULE A to CM PLACEMENT SOW #1

Candidate and Placement Site Details

Chart A: Candidate Details

School Year	# of Candidates	Grade	Subject
2026-2027	0- 25	K-12	EC-6, Bilingual EC-6, Core Subjects 4-8, 4-8 and 7-12 Core Subjects (ELAR, Social Studies, Math, Science), and Special Education
2027-2028	0- 25	K-12	EC-6, Bilingual EC-6, Core Subjects 4-8, 4-8 and 7-12 Core Subjects (ELAR, Social Studies, Math, Science), and Special Education
2028-2029	0- 25	K-12	EC-6, Bilingual EC-6, Core Subjects 4-8, 4-8 and 7-12 Core Subjects (ELAR, Social Studies, Math, Science), and Special Education
2029-2030	0- 25	K-12	EC-6, Bilingual EC-6, Core Subjects 4-8, 4-8 and 7-12 Core Subjects (ELAR, Social Studies, Math, Science), and Special Education
2030-2031	0- 25	K-12	EC-6, Bilingual EC-6, Core Subjects 4-8, 4-8 and 7-12 Core Subjects (ELAR, Social Studies, Math, Science), and Special Education

Chart B: Proposed Placement Schools

Name of School	School Year	# of Candidates
Elementary Schools Athens Elementary School Five Palms Elementary School Frank Madla Elementary School Hutchins Elementary School Kindred Elementary School Miguel Carrillo Junior Elementary School Neil Armstrong Elementary School Palo Alto Elementary School Price Elementary School Middle and Junior High Schools Abraham Kazen Middle School Alan B Shepard Middle School Dwight Middle School ● Robert C Zamora Middle School High School South San High School	2026-2027 - 2030-2031	0-25 per year

SCHEDULE B to CM PLACEMENT SOW #1

AMERICORPS PROHIBITED ACTIVITIES

Citations: 45CFR § 2520.65 –

FOR INFORMATIONAL PURPOSES ONLY:

While charging time to the AmeriCorps program, accumulating service or training hours, or otherwise performing activities supported by the AmeriCorps program or CNCS, members may not engage in:

a. Attempting to influence legislation;
b. Organizing or engaging in protests, petitions, boycotts, or strikes;
c. Assisting, promoting, or deterring union organizing;
d. Impairing existing contracts for services or collective bargaining agreements;
e. Engaging in partisan political activities, or other activities designed to influence the outcome of an election to any public office;
f. Participating in, or endorsing, events or activities that are likely to include advocacy for or against political parties, political platforms, political candidates, proposed legislation, or elected officials;
g. Engaging in religious instruction, conducting worship services, providing instruction as part of a program that includes mandatory religious instruction or worship, constructing or operating facilities devoted to religious instruction or worship, maintaining facilities primarily or inherently devoted to religious instruction or worship, or engaging in any form of religious proselytization;
h. Providing a direct benefit to—
    i. A business organized for profit;
    ii. A labor union;
    iii. partisan political organization;
    iv. A nonprofit organization that fails to comply with the restrictions contained in section 501(c)(3) of the Internal Revenue Code of 1986 related to engaging in political activities or substantial amount of lobbying except that nothing in these 9 provisions shall be construed to prevent participants from engaging in advocacy activities undertaken at their own initiative; and
    v. An organization engaged in the religious activities described in paragraph 3.g. above, unless CNCS assistance is not used to support those religious activities;
    vi. Conducting a voter registration drive or using CNCS funds to conduct a voter registration drive;
j. Providing abortion services or referrals for receipt of such services; and
k. Such other activities as CNCS may prohibit.

Individuals may exercise their rights as private citizens and may participate in the activities listed above on their initiative, on non-AmeriCorps time, and using non- CNCS funds. Individuals should not wear the AmeriCorps logo while doing so.

Exhibit 1

Data Sharing Agreement to the Teach For America Master Professional Services Agreement

This Statement of Work #2 (hereinafter called the "SOW") is issued pursuant to the Master Professional Services Agreement between Teach For America, Inc. ("Client") and South San Antonio ISD ("School Partner"), effective December 15, 2025 (the "MSA"). This SOW is subject to the Standard Terms and Conditions contained in the MSA. In the event of a conflict between this Data Sharing Agreement and the MSA, the term that is most protective of Student Records and Student Partner Data shall prevail. .

The Exhibit(s) to this SOW, if any, shall be deemed to be a part hereof. In the event of any inconsistencies between the terms of the body of this SOW and the terms of the Exhibit(s) hereto, the terms of the body of this SOW shall prevail.

RECITALS

WHEREAS, on December 15, 2025 the School Partner and Teach For America entered into separate Statement(s) of Work whereby Teach For America agreed to recruit, select, train and provide ongoing professional development to Participants and Fellows committed to closing the achievement gap by serving as effective classroom teachers specifically equipped to enhance student achievement in under-resourced school systems. As such, under 34 CFR 99.31(a) Teach For America has a legitimate educational interest in accessing and using, and (b) School Partner may share with Teach For America, the School Partner Data described herein;

WHEREAS, Teach For America desires to use the School Partner Data to track the growth and achievement of students taught by Participants and Fellows supported by Teach For America and to measure the impact of these Participants and Fellows within their contexts in order to provide: tailored support and professional development programming for these Participants and Fellows, report to funders and board members, and to evaluate and evolve our model for selecting new teachers into the program, and support School Partner in improving teacher development, effectiveness and student outcomes.

Accordingly, School Partner and Teach For America agree to be bound by the terms and conditions of this Data Sharing Agreement except that School Partner may revoke its consent to this Data Sharing Agreement at any time in its discretion..

I. DEFINITIONS

A. "Breach" will mean any actual or reasonably suspected unauthorized access, acquisition, use, disclosure, loss, modification, destruction, or inability to account for any Partner Data.

B. "Student Record Data" means and refers to the data described more fully in **Schedule A** that School Partner provides to Teach For America in connection with this DSA.

C. "Cultivate Survey Data" means and refers to data collected through Cultivate student survey via UChicago Impact 's Survey Administration Tool from students in Participant or Fellow classrooms, grades 5-12, as described more fully in **Schedule B**.

D. "Elevate Tool" refers to a Cultivate-aligned progress monitoring tool administered through PERTS to support educator development and continuous improvement as described more fully in **Schedule B**.

E. "Ignite Student Survey Data" means and refers to data collected through the Ignite Student Survey from students participating in the Ignite program as described more fully in **Schedule C**.

F. "Pencil Spaces" refers to the virtual learning platform utilized for Ignite tutoring as described more fully in **Schedule D,** while "Pencil Spaces Data" refers to all data contained therein.

G. "Partner Survey Data" individually and collectively refers to Cultivate Survey Data, using the Elevate Tool, Ignite Student Survey Data and Pencil Spaces Data

H. "Video & Audio Data" means and refers to data described as videotaping or recording of instruction or recording of the audio of in-person or virtual spaces for review of instructional technique, which are manual transferred or uploaded to Teach For America's software and servers in connection with this DSA, as described more fully in **Schedule E**.

I. "Partner Data" collectively refers to Student Record Data, Partner Survey Data, and Video & Audio Data.

J. "Aggregate Partner Data" collectively refers to de-identified Partner Data aggregated with counts of no less than 20 for internal reporting and no less than 30 for any external reporting.

K. "FERPA" means and refers to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and implementing regulations set forth in 34 CFR Part 99.

L. "PPRA" means and refers to the Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h and implementing regulations set forth in 34 CFR Part 98.

M. "Personal Data" means and refers to any information that identifies or that can reasonably be used to identify a specific individual, including but not limited to any information that meets the definition of "Personally Identifiable Information" set forth in 34 C.F.R. § 99.3

N. "Privacy and Security Laws" means and refers to (i) all applicable U.S. federal, state, and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to privacy, confidentiality, security, or breach notification of Personal Data, including but not limited to FERPA and (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security.

II. SECURITY AND SECURITY REVIEW.

A. Security. Teach For America will implement and maintain standard industry practices to protect the confidentiality, integrity, and security of all Partner Data and Student Data, including but not limited to maintaining and implementing the Security Policy at Exhibit 2. In the event that there is an update to Teach For America's Security Policy, such update shall not deprecate the level of security set forth in Exhibit 2.

B. Security Review. School Partner reserves the right to request security documentation from Teach for America, including but not limited to third-party security audit reports, security policies, responses to security questionnaires, and internal security review reports. In the event that such Security Review identifies security vulnerabilities, Teach for America will timely remediate that vulnerability.

C. Third Party Providers. Teach for America will enter into contracts with its Third Party Service Providers that require Third Party Providers to implement and maintain standard industry practices to protect the confidentiality, integrity, and security of all Partner Data and Student Data it may process or have access to.

D. Security Breaches. In the event of a reasonably suspected or confirmed security breach, Teach for America will immediately but within no later than 48 hours notify School Partner in writing. Such notification shall include a description of the systems impacted and the data impacted. Teach for America will comply and cooperate with School Partner in fulfillment of any obligations pursuant to FERPA or applicable law arising from such breach and cooperate with School Partner in an investigation regarding the security breach.

E. Data Retention and Deletion. Teach for America shall retain any Partner Data and Student Records only so far as required to provide the Services under the MSA. Teach for America shall permanently destruct any Partner Data and Student Records within 10 days of the earlier of the Termination of the MSA or the completion of the Services. This Data Retention and Data Deletion provision shall also apply to Partner Data and Student Records saved as back-up or recovery data. School Partner reserves the right to request written confirmation from Teach for America that it has permanently destroyed data in accordance with this provision.

III. DESCRIPTION OF DATA ACCESS, EXCHANGE AND USE

A. Pursuant to Partner's obligations under FERPA, and its implementing regulations as may be amended, Partner agrees that Teach For America performs an institutional service. Specifically, due to Partner's provision of Teach For America services, such as tailored support and professional development programming for Participants and Fellows, and the associated evaluation and evolution of programming offered to Participants and Fellows and the Partner, Partner agrees that Teach For America is a school official with legitimate educational interest in the disclosed Partner Data.

B. Student Record Data. Partner will provide the Student Record Data described in **Schedule A** to Teach For America in a form, format, frequency, and security feature mutually agreed by the Parties and laid forth in **Schedule A**. Access to Student Record Data at the individual student level will be limited solely to appropriate Teach For America staff and contractors. Teach For America staff will acknowledge and sign the Teach For America Information Confidentiality and Security Policy ("ICSP"). The ICSP provides guidance on processes and procedures related to the access, use, sharing, storing, and disposal of Personally Identifiable Information (PII) and student record data. Contractors and third-party programmatic data vendors, (such as Pencil, UChicago and other vendors, etc.), will sign agreements that include confidentiality provisions and be bound to the applicable process and procedures related to access, use, sharing, storing and disposal of Partner Data, PII and student record data as outlined in FERPA and PPRA as appropriate.

C. Cultivate Survey Data and Elevate Tool. Participants will receive a unique link for student survey administration through UChicago Impact's Survey Administration Tool; link will be shared with students and responses will be kept confidential and stored on secure servers. Only UChicago Impact and UChicago Consortium staff and agents necessary for administration of the survey will have access to student and teacher identifiers during administration as described in **Schedule B.** In addition, Participants may administer Elevate, a Cultivate-aligned progress-monitoring tool administered through PERTS to further support educator development and continuous improvement. UChicago Consortium access data to create Rasch benchmark scores used for reporting valid scores on teacher reports, along with analyses to improve the validity of the survey. Access to student-level Cultivate Survey and Elevate Tool Data will be limited solely to UChicago Impact and UChicago Consortium staff, Teach For America staff members, approved contractors and Participants for ongoing coaching and development of Participants and programmatic improvement.

D. Video & Audio Data. Participants will transfer or upload Partner Video and Audio Data to Teach For America in a form, format, frequency, and security mutually agreed by the Parties and set forth in **Schedule E**.

E. Teacher Evaluation Data. Partner will provide limited teacher observation/evaluation data as outlined in attached **Appendix A**. Access to Teacher Evaluation/Observation data at the identified individual teacher level will be limited solely to Teach For America regional and national staff (after Participants execute **Attachment C**).

F. No student identifiable information in the Partner Data will be reported externally; all data will be reported in the aggregate (with groups not less than 30). Partner Data may not be loaned or otherwise conveyed to anyone other than staff, current and future Participants, Fellows, and internal contractors using software services to

securely house and host this data. No student identifiable information in the Partner Data may be shared with third-party programmatic data vendors without approval via an Additional Request as outlined in Section J, below.

G. Aggregate Partner Data and Additional Uses. After creating and verifying the final merged data set, personally identifiable data shall be destroyed in compliance with 34 CFR Section 99.31 (a) (6). Consistent with FERPA, Partner agrees that Teach For America will retain and use Aggregate Partner Data to drive programmatic impact, including but not limited to developing training; improvement of services; externally sharing learnings of programmatic impact at scale, and other program strategies ("Additional Uses"). Partner also agrees that Aggregate Partner Data may be redisclosed to research institutions which support Teach For America in conducting deeper research studies ("Research Uses") and may be used with other 3rd party tools ("Additional Tools") to further improve Teach For America's program services. Teach For America will not share Aggregate Partner Data for student cohorts less than 20). Teach For America may externally share de-identified,anonymized, and aggregated analyses and conclusions that do not identify students or the Partner. Teach For America will not externally share or publish conclusions from any analyses that identifies the Partner, without the prior express written consent of Partner. Based on Partner's request, Teach For America agrees to share any findings from its analyses and/or aggregate reports with Partner.

H. Additional Requests. Teach For America may obtain additional data, use of data, or use of 3rd party data tools, surveys or systems that collect or utilize FERPA-protected data or additional shares of FERPA-protected data with third-party programmatic data vendors, via submitting written notices (an "Additional Request"), to Partner at any time, which detail the names of such parties and a brief description of such parties' legitimate educational interest in receiving such information, and an opt-out function. For the avoidance of doubt, identified FERPA-protected Partner data may only be used solely for the purposes outlined herein or providing the Services as set forth in agreed upon SOW, unless an Additional Request is approved expressly in writing and signed by an authorized representative of the the Partner. This form of notice does not entail nor require a written contract amendment; If Partner agrees to provide such data or to an additional use or share of FERPA-protected data, all terms of this MSA and this Data Sharing Agreement apply to the additional data, use of data, use of 3rd party tools or additional share. This includes ongoing data for subsequent cohort years, in which Teach For America and Partner have entered an Statement of Work or other professional service agreement, after this original DSA is signed.

IV. DUTIES

A. The School Partner will perform the following duties:

1. Provide data for the purposes of this Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232g and 34 C.F.R, section 99, and related Texas Education Code provisions.

2. Provide Teach For America with information security specifications required to transmit pupil record information electronically in the form, format, frequency, and security features laid out in **Schedule A**.

3. Pursuant to Partner's obligations under FERPA and the PPRA, Partner authorizes Teach For America and Participants, by execution of this Agreement, to administer Cultivate, Elevate, or Ignite student surveys to

students in Participant or Fellow classrooms or those engaging in Teach For America programming in the form, format, frequency and security features laid out in **Schedule B and Schedule C**.

4. Authorizes Teach For America to enter emails and names of students participating in Ignite tutoring into the Pencil Spaces web-based software for rostering and tutoring administration. Authorizes Teach For America's Fellows to record instruction in in-person or virtual spaces for review of instructional technique.

5. Authorizes Teach For America's Participants to record instruction in in-person or virtual spaces for review of instructional technique except that Teach for America Participants will comply with any restrictions, instructions, directives, rules, procedures, or policies of the District regarding any recordings. In the event of a conflict between the District's restrictions, instructions, directives, rules, procedures, or policies of the District and Teach for America instruction regarding recordings, the District's restrictions, instructions, directives, rules, procedures, policies, shall prevail.

6. Unless otherwise prohibited or restricted by law, Partner specifically names Teach For America as an approved affiliate or partner and third-party beneficiary of the Partner with regard to all parental permission/releases previously signed by students and/or parents as they relate to the collection of student record data, survey data, recording video and audio data from/of students. Further, if required by FERPA, the PPRA or state law, Partner will provide reasonable updated notices to parents, or students of appropriate age, related to surveys, video or audio recordings, obtain consent for same, and/or offer an opportunity for parents, or students of appropriate age, to opt-out of participating in said surveys, video or audio recordings.

B. Teach For America will perform the following duties:

1. Comply with all FERPA and PPRA Texas Education Agency Provisions. Teach For America agrees to require all staff members, contractors, or agents to comply with this provision.

2. Partner may require Teach For America to provide documentation of Teach For America's information security specifications prior to data transmittal.

3. Teach For America shall designate an authorized representative able to request data under this agreement. The authorized representative shall be responsible for transmitting all data requests, confirmation of the completion of any projects and the return or destruction of data.

4. In the event of a Breach, Teach For America shall notify the Partner in accordance with FERPA, and/or any applicable state law or regulation to manage the Breach without unreasonable delay and within no later than 48 hours. Teach For America shall also cooperate with the Partner with regard to management and response of any such Breach.

V. SPECIAL TERMS AND CONDITIONS OF SOW #2

A. *Term*. The Term of this Agreement shall begin on the Effective Date, and shall only cover Participants, Fellows and Facilitators whose engagement with the Partner begins during the school years 2026-27, 2027-28, 2028-29, 2029-30, 2030-31. All provisions of this DSA shall be valid from the date of execution through June 1, 2031

(the "Expiration Date"). While this Agreement shall expire on the Expiration Date, all sharing arrangements shall be valid until such time the named cohorts of Participants, Fellows and Facilitators have completed their applicable term of engagement.

B. *Termination.* This Data Sharing Agreement may be terminated as follows:

1. At any time by mutual agreement of the parties;
2. By either party upon thirty (30) days prior written notice to the other Party;
3. By either party upon written notice to the other in the event of a material breach of this Agreement that is not cured within thirty (30) days following the receipt by the breaching party of written notice from the non-breaching party.

C. *Effect of Termination*. If this SOW expires or is terminated by either party, it shall become void. The expiration or earlier termination of this specific SOW shall not serve to terminate the associated Master Service Agreement or any other SOW.

D. *Notices*. Any notices to either Party under this Data Sharing SOW shall be in writing and delivered by hand or sent by nationally recognized messenger service, or by registered or certified mail, return receipt requested, to the addresses set forth below or to such other address as that Party may hereafter designate by notice. Notwithstanding the foregoing, security breach notifications shall also be sent immediately by email to: the District's Technology Director

SOUTH SAN ANTONIO ISD DATA CONTACT

Name: _____

Title: _____

Address: _____

Email: _____

	TEACH FOR AMERICA:		With an electronic copy to:
Name:	Dana Nguyen	Name:	TFA Legal Affairs
Title:	Director, Data Analytics	Email:	LegalAffairs@teachforamerica.org
Address:	3555 Timmons Ln #800, Houston, TX 77027		*Send only notices related to breach of contract and indemnity.
Email:	Dana.Nguyen@teachforamerica.org		

E. *Technical Contacts.* The points of contact for technical issues regarding the exchange, storage and security of the

School Partner Data and related technical issues are:

South San Antonio Public Schools	Teach For America
Name:	Name: Dana Nguyen
email:	email: Dana.Nguyen@teachforamerica.org
Phone:	Phone: (713) 523-4100

F. *Authority*. This Data Sharing Agreement supersedes all communications between the parties related to the subject matter of this SOW.

Exhibit 1 - ACCEPTANCE FOLLOWS

IN WITNESS WHEREOF, each of School Partner and Teach For America has caused its duly authorized representative to sign this Statement of Work #2 re Data Sharing Services in the space provided below.

South San Antonio Independent School District		Teach For America	
By:		By:	
Name:	Dr. Saul Hinojosa	Name:	Nick Garcia
Address:	1450 Gillette Blvd San Antonio, TX 78224	Title:	Executive Director
		Address:	1209 S. St. Mary's St. San Antonio, TX 78210

SCHEDULE A to Exhibit 1 re Data Sharing

Data Elements, Form, Format, Frequency and Security Features

Partner will, to the fullest extent possible, include the following data and specified variables in the Partner Data sets provided to Teach For America (limited only by what is available through the method of access);

a. The following program participant data and variables are essential to Teach For America's data request:
   i. district, district NCES code, school, school NCES code, staff unique identifier (ID)
   ii. Subject name, course name, course ID, section ID

b. The following program participant data and variables are helpful but not essential to Teach For America's data request:
   i. years employed with partner
   ii. Teach For America affiliation (current CM/ alumni/ fellow)
   iii. certification/ license level
   iv. gender
   v. race
   vi. ethnicity
   vii. teacher evaluation rating/ observation data (where available). Notwithstanding the foregoing, the District is not obligated to provide copies of any of if its internal evaluation records or to provide any records from District's HR files. Though, the District will provide TFA-specific evaluation forms.
   viii. student/parent survey summary results (where available)

c. The following student data and variables are essential to Teach For America's data request:
   The District will provide aggregate and summary data but will not provide individually identifiable student records.
   i. interim assessment scores (BOY, MY, EOY) (all scores including growth goals/targets, grade level equivalency, scale scores, percentile rank, or other scales available)
   ii. previous and current year state test scores (all scores including scale score, proficiency/ performance level, percentile rank, growth met, student growth percentile, or other scales available)
   iii. student survey results (all scores including individual question scores, aggregate construct scores, raw scores, any deidentified open ended responses or other scales available)
   iv. test subject
   v. test year

vi.

   vii. grade level
   viii. race/ ethnicity
   ix. ELL status
   x. special education/ disability status
   xi. low socioeconomic-status (SES)
   xii. days present in school
   xiii. days enrolled in school

d. The following aggregate data are essential to Teach For America's data request:

i. Partner average scores for all interim assessment tested grades and subjects (all scores including growth goals/targets, grade level equivalency, mastery, percentile rank, or other scales available)
ii. Partner average scores for all state tested grades and subjects (all scores including scale score, proficiency/ performance level, raw scores, percentile rank, or other scales available) tested grades and subjects (all scores including scale score, proficiency/ performance level, raw scores, percentile rank, or other scales available)
iii. Partner average scores for all [student survey] surveyed grades and subjects (all scores including individual question scores, aggregate construct scores, raw scores, any deidentified open ended responses or other scales available)

Data Security

Teach For America employs a number of strategies to secure data and limit unnecessary access during transfer, storage, and processing. We encrypt data in transfer as well as at rest when it is being stored in a data repository. For our internal data storage, we change encryption keys on a regular basis to avoid stale credentials and unwanted legacy access. Data is regularly obfuscated for analytics and reporting purposes. We use best practices for data isolation, including limiting accounts for vendors who push data to our systems and centralized oversight of user accounts for external systems when we need to pull the data ourselves. We use a "least privilege granted" model for access to internal systems, employing multi-factor authentication, and monitor access across these systems with auditable logs. Additionally, we have blanket data privacy training for all staff that covers key elements of working with PII, sensitive data, and student data.

Teach For America shall also have a written incident response plan, which shall include but is not limited to, prompt notification to Partner within 48 hours in the event of a security or privacy incident, as well as procedures for responding to a breach of any of Partner's Data or Student Data that is in Teach For America's possession. Teach For America agrees to share its incident response plan upon request.

SCHEDULE B to SOW #2 re Data Sharing

Description of System(s) Used in the Transfer of School Partner Survey Data, frequency and Security Features

System Description:

Cultivate Description:

This **Schedule B** shall serve as Teach For America- San Antonio's official notification of the use of the Cultivate for Coaches student survey for professional development and organizational reporting. A joint program of UChicago Impact and UChicago Consortium, Cultivate for Coaches is a professional development program designed to support coaches and Participants in creating learning environments that positively affect what students believe about themselves as learners and the strategies they employ in their classrooms, ultimately improving student academic performance. This program includes student surveys for grades 5-12 administered by UChicago Impact. The survey is crucial because it will provide Participants with important information on students' perceptions of the classroom learning environments that, in turn, can support their understanding of strengths and areas of growth. Below we've outlined the various ways Teach For America- San Antonio and Participants will utilize Cultivate student survey data, including but not limited to:

- Participants review student feedback to prioritize areas for growth.
- Coaches utilize data to support individual teacher development, based on evidence from student surveys, and incorporate evidence-based best practices provided by University of Chicago.
- Teach for America reports aggregate data as a key performance indicator for continuous improvement of programmatic supports.

Cultivate Survey Security Features:

UChicago Impact will administer the Cultivate for Coaches Survey to students of Teach For America. Participants in grades 5-12. The surveys will be administered using UChicago Impact's Survey Administration Tool. Each teacher will receive a unique link for student survey administration.

- Student identification will be kept confidential and stored on secure servers for both outreach and survey administration. Only UChicago Impact and UChicago Consortium staff and agents necessary for administration and reporting of the survey will have access to student and teacher identifiers during administration.

- Students will select their birthdate, gender, grade level, school and teacher using a combination of drop-down lists or radio buttons. This data is collected solely for the purposes of reconciling multiple surveys from the same students. Students have the right to omit responses to any question. Once data collection and reporting are complete, student identifying information will be permanently deleted.
- Students will also have the option of selecting their race/ethnicity in order for Teach For America to understand how student perceptions vary by race/ethnicity.
- To receive student data, CMs must have at least 50% of students (based on student count provided by Teach For America) complete the survey and have at least 5 valid respondents per item to receive full report data. Partial survey responses will also be accepted.
- Only aggregate data (for classrooms with at least 5 students) will be reported to teachers on a password-protected basis.
- TFA will have access to student-level data without any identifiable information through a password-protected system.
- UChicago Impact shall keep all non-identifiable student scores for national benchmarking purposes but cannot report on any aggregate results without explicit permission from Teach For America.
- UChicago Impact employs several industry standard practices to secure data and prevent unauthorized access. Data is encrypted both while in transit during the survey process, and while at rest when stored in the data repository. Encryption keys are changed on a regular basis to avoid stale credentials and unwanted legacy access. Data is regularly obfuscated for analytics and reporting purposes and is aggregated by being rolled up at the classroom, instructor, school or district level. The server management team enforces data isolation and oversight of all user accounts accessing data, including continuous monitoring of access across our systems using centralized, auditable logs.

System Description:

Elevate Description:

This **Schedule B** shall serve as Teach For America-San Antonio's official notification of the use of the PERTS Elevate as an optional progress monitoring tool for professional development and continuous improvement. Elevate is designed to be used in conjunction with Cultivate for Coaches to support educator development and continuous improvement. It is fully aligned with the classroom condition questions included in the Cultivate survey. It is customizable based on educator needs and is intended to be administered anywhere from one to four times a year, in between Cultivate fall and spring administration. It takes approximately 5-10 minutes for students to complete. Administration and reporting are designed to give educators immediate insight on the classroom conditions they are prioritizing for improvement.

Elevate Survey Security Features:

- Participants that opt into Elevate will receive a unique link for each class that participates in student survey administration. Participants will include students email addresses so that each student receives a unique survey link. This is solely for the purposes of restricting duplication in the survey responses from the same

students.

- Students have the right to omit responses to any question. Once data collection and reporting are complete, student identifying information will be permanently deleted.
- Student identification will be kept confidential and stored on secure servers. Only PERTS staff and agents necessary for administration of the survey will have access to student identifiers. PERTS will delete all PII within one year.
- Only aggregate data (for classrooms with at least 5 students) will be reported to teachers on a password-protected basis.
- Teach For America staff will have access to aggregate data. If Teach For America requests access to student-level data for programmatic improvement purposes, data will not contain any identifiable student information and will only be available to staff through a password protected system.
- PERTS has the right to keep all non-identifiable student scores for national benchmarking purposes but cannot report on any aggregate results without explicit permission from Teach For America.
- PERTS employs a number of industry standard practices to secure data and prevent unauthorized access. Data is encrypted both while in transit during the survey process, and while at rest when stored in the data repository. Encryption keys are changed on a regular basis to avoid stale credentials and unwanted legacy access. Data is regularly obfuscated for analytics and reporting purposes and is aggregated by being rolled up at the classroom, instructor, school or district level. The server management team enforces data isolation and oversight of all user accounts accessing data, including continuous monitoring of access across our systems using centralized, auditable logs.

SCHEDULE E to Data Sharing Agreement

DESCRIPTION OF SYSTEM(S) USED IN THE TRANSFER OF PARTNER VIDEO & AUDIO DATA, FREQUENCY AND SECURITY FEATURES

System Description:
Video & Audio Storage Systems Description:

This **Schedule E** shall serve as Teach For America-San Antonio's official notification of the use of video and audio storage for corps member teacher coaching and training. Below we've outlined the various ways Teach For America- San Antonio and Participants will utilize the video and audio storage platform, including but not limited to:

- Uploading and reviewing classroom recordings and other content to engage in discourse and feedback on teaching practices.
- Foster strong dialogue and collaboration with other Participants and Teach For America staff as they share resources, ideas, and feedback.
- Streamline coaching conversations centered on individual teacher development, rooted in evidence from their classrooms, and use evidence-based practices modeled by other teachers.

As part of our use of classroom video and audio, Teach For America Participants will be uploading their classroom recordings. Although the video recordings are focused and framed around the teacher, there may be times they include student images.

Video and Audio Storage Security Features:
Although Participants will upload classroom recording videos and audio, these recordings are not sharable outside of the platform and only the corps member who uploaded the recording and Teach For America coaches have rights to download it. Data is encrypted in transfer as well as at rest when it is being stored in the data repository. We use a "least privilege granted" model for access to internal systems, employing multi-factor authentication where feasible, and monitor access across these systems with auditable logs.
Our video and audio storage platform meets rigorous data security and privacy standards as a closed and private platform and complies with laws and regulations concerning the privacy, security, and notification of breaches.

Exhibit 2

The following table is an overview of the security controls implemented by Teach For America, organized by the 23 categories of the NIST Cybersecurity Framework.

For context, we used version 1 of the NIST Cybersecurity Framework as guidance when developing our cybersecurity program, modeling our actions after the framework's recommended process for establishing or improving a cybersecurity program described in section 3.2:

- The Security and Compliance team members determined TFA's current profile by reviewing each of the subcategories of the NIST Cybersecurity Framework and documenting whether or not each subcategory had a corresponding policy, procedure, technology and person.
- The Security and Compliance team members then determined what the desired state should be for each NIST Cybersecurity framework subcategory, and developed action plans to address the gaps that surfaced.

Function	Category	TFA Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	All data is secure in OneDrive, SharePoint, Azure Cloud or Google Drive. Identities are secured with Azure MFA. Laptop assets are managed by the Endpoint team and hard drive disks are encrypted. Network hardware assets are managed by the Network Platform team.
IDENTIFY (ID)	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Teach For America's technology teams align our goals and priorities with the organization and provide quarterly reporting/updates to ensure the continued alignment of our goals. We go through a rigorous goal review to ensure alignment at the subteam level. The Security team aligns its goals with those of the organization and technology subteams.

IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	The Security team is responsible for managing technology risks and reports into the Legal teams Risk and Compliance subteam. In partnership with Legal, Data Privacy and Risk & Compliance teams, we ensure risks are analyzed, assessed and appropriately mitigated. The Security team manages and updates all risks including cybersecurity risks through Confluence in our Technology Risk page and with Jira tickets.

Function	Category	TFA Response
IDENTIFY (ID)	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	The Security team follows a Enterprise Risk Methodology provided by the Risk & Compliance team to assess, score, manage and remediate all risks. All risks are documented and reported on to Technology team leaders and the Risk & Compliance team who then shares the information with our Board.
IDENTIFY (ID)	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	The Security team follows a Enterprise Risk Methodology provided by the Risk & Compliance team to assess, score, manage and remediate all risks. All risks are documented and reported on to Technology team leaders and the Risk & Compliance team who then shares the information with our Board.
IDENTIFY (ID)	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented processes to identify, assess and manage supply chain risks.	The Security team follows a Enterprise Risk Methodology provided by the Risk & Compliance team to assess, score, manage and remediate all risks. All risks are documented and reported on to Technology team leaders and the Risk & Compliance team who then shares the information with our Board.

PROTECT (PR)	Identity Management, Authentication and Access Control (pr.ac - This is a premium name): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Teach For America is mature regarding this control. Our data center is hosted by Microsoft Azure and so access to our most critical data and systems is restricted and limited. Access to network lan closets located in some regional offices is restricted to specific staff members in the office.
PROTECT (PR)	Awareness and Training (Definition von Public Relations (PR) | PR.at): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	The Teach For America security team requires cybersecurity training annually for all staff and contractors. We also perform several phishing exercises each year. In addition to the cybersecurity training, we recently required all staff and contractors take a specific Business Email Compromise phishing training.

Function	**Category**	**TFA Response**
PROTECT (PR)	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	The Teach For America Security and Legal teams partner closely regarding data security. The Legal team manages the Information Confidentiality and Security Policy or ICSP which includes guidance regarding proper data handling responsibilities. All staff are required to take specific ICSP training.

PROTECT (PR)	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	The Teach For America Technology team updates staff facing policies twice each year. Included in these policies is the Technology Acceptable Use Policy.
PROTECT (PR)	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	N/A. Teach For America does not own or operate Industrial or Operational Tech.
PROTECT (PR)	Protective Technology (pr.pt is for sale!): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Yes, through our SIEM and Microsoft security tools we are thoroughly protected in this area. For example, our SIEM gives us the capability of centralized log collection from endpoints, servers, network devices, Azure Cloud and Cloud Apps.
DETECT (DE)	Anomalies and Events (SSD Hosting in Deutschland bei InterNetworX): Anomalous activity is detected and the potential impact of events is understood.	We have 24/7/365 Security Operations through Rapid7 Managed Detection and Response or MDR. Included with that service is InsightIDR, their next-gen SIEM solution. With InsightIDR and Microsoft Defender EDR, it gives us the capability to detect and respond to suspicious and malicious activity. And the Security team continues to refine and mature our monitoring and operations process over the past two years since implementation of Rapid7 MDR in the Fall of 2023.

Function	Category	TFA Response
DETECT (DE)	Security Continuous Monitoring (subdomain.com - Subdomain.com): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	We have 24/7/365 Security Operations through Rapid7 Managed Detection and Response or MDR. Included with that service is InsightIDR, their next-gen SIEM solution. With InsightIDR and Microsoft Defender EDR, it gives us the capability to detect and respond to suspicious and malicious activity. And the Security team continues to refine and mature our monitoring and operations process over the past two years since implementation of Rapid7 MDR in the Fall of 2023.
DETECT (DE)	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	We have monthly meetings with our Rapid7 cybersecurity advisor as part of our MDR service and we review and maintain our detections on that call.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Teach For America has a thorough and mature Incident Response plan. Our IR plan has been reviewed and revised three versions over and vetted by external assessors. We have also run multiple tabletop exercises with business teams across the organization testing our processes and communications. We identified gaps and remediated them with the aforementioned plan revisions. The TFA Security team documents and updates all of their SecOps

		runbooks. We review alert notifications and escalation to ensure our incident response capabilities are optimal.
RESPOND (RS)	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Teach For America has a thorough and mature Incident Response plan. Communications and escalation across the technology team, business teams and our managed detection and response external partner is documented and well known.
RESPOND (RS)	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Teach For America has a thorough and mature Incident Response plan. Communications and escalation across the technology team, business teams and our managed detection and response external partner is documented and well known.

Function	Category	TFA Response
RESPOND (RS)	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	As part of our Incident Response plan we create a root cause analysis report and run a postmortem meeting with all of the critical teams involved in any incident. Identified gaps are documented and added to our remediation plan.
RESPOND (RS)	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	As part of our Incident Response plan we create a root cause analysis report and run a postmortem meeting with all of the critical teams involved in any incident. Identified gaps are documented and added to our remediation plan.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Teach For America has a thorough and mature Incident Response plan. Our IR plan has been reviewed and revised three versions over and vetted by external assessors. We have also run multiple tabletop exercises with business teams across the organization testing our processes and communications. Our Backup solution is in the Cloud using Azure Backup and is tested monthly. Our infrastructure is entirely in Microsoft Azure and we are able to build resiliency into all of our critical assets.

RECOVER (RC)	Improvements (Investment Management | Stockbroking Services | Private Wealth Management | Isle of Man): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Teach For America has a thorough and mature Incident Response plan. As part of our Incident Response plan we create a root cause analysis report and run a postmortem meeting with all of the critical teams involved in any incident. Identified gaps are documented and added to our remediation plan. Cybersecurity assessments and tabletop exercises are run regularly and areas for improvement are documented and added to a remediation plan.
RECOVER (RC)	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendCommunications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). ors).	Teach For America has a thorough and mature Incident Response plan. Our IR plan has been reviewed and revised three versions over and vetted by external assessors. We have also run multiple tabletop exercises with business teams across the organization testing our processes and communications. We identified gaps and remediated them with the aforementioned plan revisions.

Teach For America

Cyber Incident Response & Communication Plan

Author: [Security & Compliance]

Teach For America

Document Version Control

a. Document History

The following table records information regarding released versions of this document and briefly describes the changes made to them.

Version	Date	Author	Comment / Changes from Prior Version
1.02	January, 2021	Harpreet Bajwa and Tara Thomas	Initial Version
2	11/xx/2022	Sulaiman Jalloh	
2.1	10/2023	Mark Desimini	

b. Document Reviewers/Approvers

Name	Position (e.g. Director-Recruitment, Project Manager, etc.)	Reviewer (only)	Reviewer and Approver
Ryan Riggin		X	
Clive Nelson III		X	
Mark Desimini			X

Teach For America

Table of Contents

Governance

- Purpose

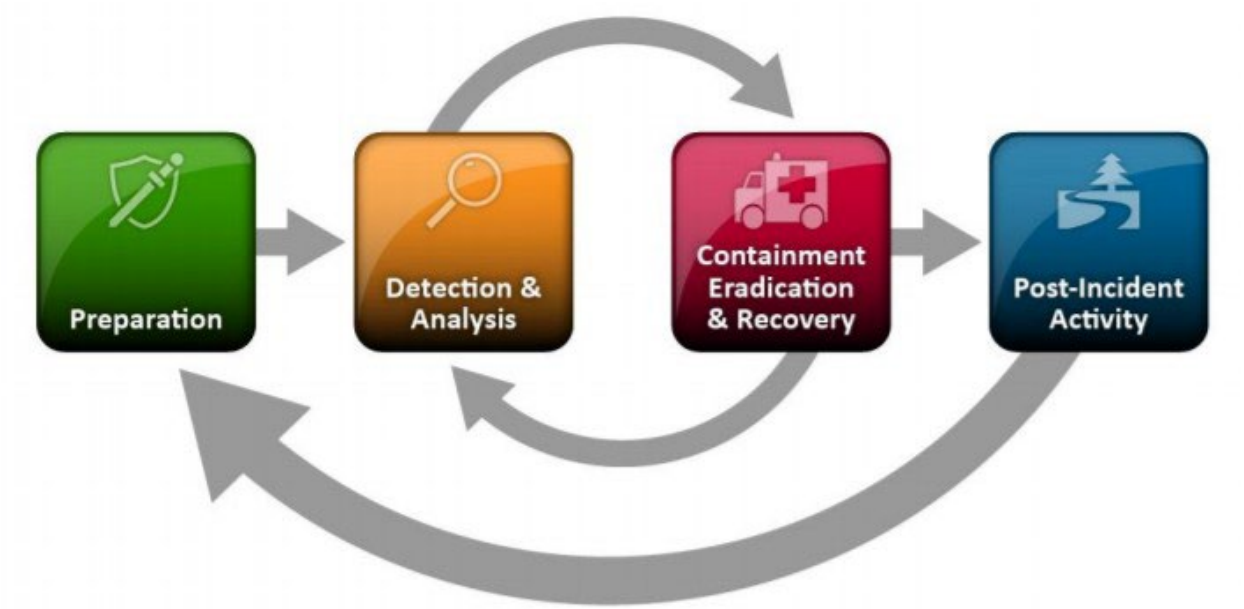
  The purpose of the Cyber Incident Response & Communication Plan is to provide Teach ForAmerica with a central capability for detecting, responding, reporting, and remediating cybersecurity incidents and for communicating during a cybersecurity incident. It has been established in order to reduce and/or minimize the impact to Teach For America networks, systems, users or business processes.

- Objective

  The objectives of the Cybersecurity Incident Response & Communication Plan:

  - Implement a structured and consistent framework for the central monitoring, coordination, and response of all cybersecurity incidents
  - Outline processes and methodologies used for managing and handling cybersecurity incident response activities
  - Ensure the timely exchange of information within the Cyber Incident Response Team and between the relevant parties across the organization
  - Comply with Teach For America policies and standards for cybersecurity incident response and any applicable regulatory requirements
  - Follow the TDX Major Incident Response process and communication procedures

  The Cybersecurity Incident Response Framework consists of operational and management sections, as illustrated in the diagram below. This Incident Response & Communication Plan is also aligned with leading cybersecurity incident response practices, including the National Institute of Standards and Technology's (NIST) guidelines (SP 800-61).



Operational Model

- Definitions

The operational model provides Teach For America with criteria for defining an event, alert or cybersecurity incident.

The table below defines the terms used in an escalation process from event to incident:

Term	Definition
Event	An event is any occurrence involving an information system on the Teach For America network. This includes logical events such as observable network traffic, user logins, vulnerability scans, etc. It also includes events which are not directly observed such as reports of stolen equipment, reports from outside regarding attacks in which Teach For America might have been involved, and user reports regarding service quality issues for certain critical resources.
Alert	An alert is triggered by a notable event or combination of events which may signal that a cybersecurity or computer security incident has occurred or is ongoing. Alerts may be received from current security detection tools and other network and host-based monitoring apparatus. Alerts may also be received in the form of reports from users, outside organizations, or threat intelligence providers.
Cybersecurity Incident	A cybersecurity or computer security incident is any event, sequence of events or indicators which threaten or compromise the confidentiality, integrity, or availability of the Teach For America information or information systems. Cybersecurity Incidents typically involve a violation or imminent threat of violation of Teach for America policies and standard security practices, requiring activation of the Cybersecurity Incident Response Team (CIRT) for response actions.

- Incident Classification & Severity
  - *Cybersecurity Incident Categories*

The classification of incidents helps determine the response priorities and resource allocation. Because incidents can occur through a wide variety of methods and attack vectors, categorization of incidents may be associated with more than one of the incident types. Below is the list of Teach For America incident categorizations:

Incident Type	Definition
Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting Teach For America digital resources.
Data Exfiltration	A successful attempt is made to remove data from the Teach For America environment without proper authorization.
Data Breach	An incident in which Teach For America highly confidential information has been accessed or exfiltrated. Highly sensitive information is defined in Teach For America Information Confidentiality & Security Policy as: *Confidential Data.*
Hacking	An event in which access gained through the misuse of legitimate user credentials (password stolen/cracked), unauthorized access to inappropriately classified or protected Teach For America sensitive information by legitimate users, and access gained through software or hardware exploitation.
Insider Threat	Any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems and uses their authorized access or understanding of an organization to harm that organization.
Misuse/ Improper Usage	The use of organizational resources in a manner or purpose other than for what it was intended. Misuse differs from Hacking in that the user was given permission or access.
Malware	Malware includes viruses, Trojans, worms, rootkits, and malicious scripts. Incidents of this type should generally only be declared in the case of malware which is not detected and/or handled by antivirus software.
Ransomware	A form of malware designed to encrypt or destroy files on a device and decrypted in exchange for ransom. Threat actors also commonly threaten to share data publicly or sell if ransom is not fulfilled.
Unauthorized Access	An individual gains logical or physical access to a Teach For America network, system, application, data, or other resource without permission.
Vendor/ Third Party	A successful attack upon a Teach For America technology vendor/ Third Party that compromises Teach For America systems or information.
Social Engineering	The practice of manipulating legitimate users into performing malicious activities using misdirection, deception, and coercion. It may be used to obtain privileged information about information systems or users, gain unauthorized access to physical locations, or to convince a user to perform an action which enables unauthorized access to an information system. It may take the form of specially crafted emails (phishing attacks), targeted phone calls/ text messages to privileged users, or deceptive face to face encounters.

Incident Type	Definition
Other	Other includes incidents that may not meet the criteria to be labeled as one of the above incident types.

- *Cybersecurity Incident Severity*

Declaring the Severity Rating of an incident is an important decision point in the initial steps of the cybersecurity incident response process. Due to resource limitations and incident impact, cybersecurity incident response efforts need to be prioritized based on the risk and level of impact that the cybersecurity incident poses to Teach For America.

A "Cybersecurity incident severity rating" should not be confused with an "alert urgency".

Cybersecurity Incident Severity Rating: summarizes risk posed to the organization and indicates the level of effort best suited for responding to a given threat. Cybersecurity Incidents typically involve a violation or imminent threat of violation of TFA's policies or standard security practices. It is applied after an alert or set of alerts have been confirmed as a cybersecurity incident. During the course of cybersecurity incident response the initial applied severity rating may need to be revisited for escalation or de-escalation using the Early Triage and Impact Assessment document.

The ratings below follow the leading practices that address confidentiality, integrity, and availability:

Severity Rating	equired Roles	Examples
High	IR Manager IR Coordinator Communication s lead Scribe	A large number of users are affected and/or not able to do their job · Widespread malware infection affecting High Value Assets (HVA) or Business Critical systems as defined in the Production System Contact List · Outage of any HVA or Business Critical for more than 10 business days as a result of a cyber attack Denial of service attack on critical infrastructure Organization is no longer able to provide some critical services to any users Ransomware infection of an HVA · Recovery from the incident is not possible without external support (e.g., sensitive data exfiltrated and posted publicly) · Compromise of a third party with high privilege access to Teach For America environment · Any incident that may have a significant impact on Teach For America's reputation Access or exfiltration of Teach For America confidential information
Medium	IR Manager Scribe	· Time to recovery is predictable with existing resources · Minimal effect; the organization can still provide all critical services to all users but has lost efficiency Malware sample that has the capability to spread to other machines

Severity Rating	Required Roles	Examples
		· Infection of 3-5 machines or more machines with known malware
Low	Security Operations Analyst	Random phishing attempts to Teach For America users · Infection of up to 1-2 machine(s) with known commodity malware, identified but not quarantined by antivirus Limited availability to a few non-critical systems External brute force attempt that does not result in successful access Unauthorized internal port scan activity

- Roles & Responsibilities

  The Cybersecurity Incident Response Team (CIRT) serves as a critical component in the support of the day-to-day operations of the Cybersecurity Incident Response Plan. The CIRT can have as many as 3 sub-teams: Senior Leadership Team, Core Team, and Extended Team. The Core Team is comprised of a group of cybersecurity incident response subject matter resources. The Extended Team provides support throughout the response process. If external assistance is required for any severity rating, third parties will be engaged.

  - *Senior Leadership Team*

    The Leadership Team can be comprised of the Chief Digital and Technology Officer (CDTO), or another VP from TDX, and at least two other members from the Leadership Team in addition to members of their teams that may act as backups their respective teams. In the case of an absence, a single member of the Leadership Team can make decisions for the entire group. This team is engaged only during high incidents. Their roles and responsibilities include the following:

Leadership Team	
Role	**Responsibility**
Leadership Team	Provides executive oversight to the response process Responds to notices of potential critical incidents and data breaches from the IR Manager • Receives incident assessment and recommendations from the Cybersecurity Incident Response Team and make decisions when prompted • Provides guidance to the Cybersecurity Incident Response Team and supports teams based on the diagnosis and recommendations • Approves communication with the Office of General Counsel & Risk, external council or external law enforcement, if necessary Communicates to Corporate and Operational Business Leadership, as appropriate • Approves communications with third parties as necessary (e.g. Law Enforcement, External Counsel) • Communicates to Teach For America executive leadership (e.g. Chief Financial Officer, EVP Talent & Operations, and Chief People Officer)

Leadership Team Members	
Role	**Responsibility**
Chief Financial Officer	Provide overall understanding of any financial impact of a cyber-incident to ensure response is appropriate given these impacts.
Chief Digital & Technology Officer	Providing overall direction, guidance, leadership and support for the cyber incident responses including deciding when to deactivate mission-critical systems or email.
Chief People Officer	Ensure we are taking a people first approach and the needs of our impacted people are front and center in our decision-making.
EVP, Talent & Operations	Ensures incident response team is engaging the right people at the right times (including the Management Team as well as Board)
General Counsel & Chief Risk Officer	Ensures we evaluate the level of risk appropriately, deciding among containment/preservation strategies in light of the potential impact on operations and our legal obligations, and complete the necessary reporting to constituents, third parties, law enforcement agencies and agencies as required.
Head of Marketing and Communications	Ensures we are communicating with the right people at the right times by crafting incident communications strategy to ensure all constituents get the appropriate information. Coordinating communications with third parties (e.g., corps members, members of the public, etc.). Making media/public statements (depending on sensitivity).

- *Core Team*

Teach For America's Security & Compliance Team acts as the primary response team for incidents and make up the Core Team. Roles designated with an (*) are only assigned on an as needed basis. Personnel may be assigned more than one role at a time. The incident manager has the authority and discretion to create and assign additional roles. Roles such as a coordinator, scribe or communications lead may need to be assigned depending on the severity and complexity of the incident. The team's roles include the following:

Core Team	
Role	**Responsibility**
IR Coordinator*	**The IR Coordinator is a position that is assigned at the time of a High severity incident. The IR Coordinator assumes the role of Communications Lead in the event of a high incident.** The IR Coordinator is the primary point of contact to ensure an incident is properly completed from notification to lessons learned. The role is assigned at the time of an incident and is responsible for directing response activities, assigning roles, and determining the need for technical/management calls. The IR Coordinator's responsibilities include the following: Direct containment and remediation tasks Chair the Technical Bridge

Core Team	
Role	**Responsibility**
	• Determine the need to engage the Office of General Counsel, People Team, Communications or other teams, as required Determine when incident is closed Chair lessons learned session
IR Manager	**The IR Manager is a position that is assigned at the time of a Medium or High severity Incident. The IR Manager provides process management support and guidance for response efforts.** The IR Manager responsibilities include the following: • Initiating Cybersecurity Incident Response Team calls and establishing zoom bridge conference numbers • Assigning specific roles that are only activated during a high or greater incident (e.g. IR Coordinator, Communications Lead, and Scribe) • Assigning multiple IR Managers if additional resources are required for managing the response process Providing expert technical input to containment, eradication, and recovery plans Chairing the technical bridge Sharing the lessons learned action items with the Cybersecurity Incident Response Team Tracking progress of remediation tasks Reporting findings Submit requests to the Consulting POCs
Communications Lead*	**The Communications Lead is a position that is assigned at the time of a High severity Incident. The Communications Lead ensures that communication requirements are met.** They will work closely with the IR Coordinator or IR Manager to provide updates to the different teams and consult with Leadership and the Office of General Counsel & Risk when crafting communications to external entities. The Communications Lead's responsibilities include the following: Communicating incident status Establishing management communication updates • Ensuring that communications are sent and coordinated properly and that communication requirements are met Directing all communication activities and communicating incident status • Providing updates and consulting with Leadership, Communications, and the Office of General Counsel & Risk team when crafting communications to external entities

Security Operations Analyst(s)	**The Security Operations Analyst(s) carries out technical cybersecurity incident response activities as directed by the IR Coordinator or IR Manager for Medium and High severity Incidents. But is the sole resource for low severity incidents.** The Security Operations Analyst's responsibilities include the following: Escalating the security alerts as per the defined alert urgency* Coordinating Managed Security Operations support with consulting points of contact (POC)*

Core Team	
Role	**Responsibility**
	Submitting requests to update security monitoring tool alerts to detect latest threats* Executing tasks that are assigned by the IR Coordinator or the IR Manager Updating to incident management tracking tool Responding to incidents escalated by departments external to Security Operations Compiling the lessons learned notes for the IR Coordinator or IR Manager
Scribe*	**The Scribe is only assigned during a High incident** and as needed for other priorities and is responsible for maintaining incident documentation and reporting. The Scribe's responsibilities include the following: Proper documentation of the incident Drafting initial notification,lessons learned summary, and the Full Incident Report

- *Extended Team*

The Extended Team is responsible for providing support to the Cybersecurity Incident Response Team during an incident. These teams will provide input and updates to the IR Coordinator or IR Manager, as necessary. The Extended Team can consist of the following Teach For America representatives:

Extended Team	
Team	**Responsibility**
Application Services Platform	Provides technical support to the Core Team in relation to Teach For America on premise application platform services inclusive of Middleware applications: Tomcat, Active MQ, Reporting solutions: BobJ, Developer Tools: Jira, Confluence and Jenkins.
Cloud Platform	Provides technical support to the Core Team in relation to Teach For America deployment, consumption, governance and management of cloud PaaS and IaaS resources (e.g., Azure, Github, etc.).
Collaboration & Communications	Provides technical support to the Core Team in relation to Teach For America collaboration & communication technologies within the landscape (e.g., Zoom, Slack, Box, Email, Teams, SharePoint, etc.)
Data Storage Platform	Provides technical support to the Core Team in relation to Teach For America data storage for transactions and analytics (e.g., SQL, Datalake, NoSQL, PowerBIetc.).
Data Privacy	Provides support for incidents involving data privacy violations response.
Engineering COE	Provides technical support to the Core Team in relation to Teach For America critical custom applications including TFA One App, TGL and Applicant Portal.
ERP Platform	Provides technical support to the Core Team in relation to Teach For America ERP platform that supports the People and Finance teams (e.g., Workday).

Extended Team	
Team	**Responsibility**
Identity Platform	Provides technical support to the Core Team in relation to Teach For America identity, authentication and access management for Staff and Non-Staff (e.g., Azure Active Directory, Tivoli Directory Services, Okta, MFA etc.).
Legal Affairs	Responsible for initiating communication with Law Enforcement and External Counsel, if necessary.
Network Platform	Provides technical support to the Core Team in relation to Teach For America network appliances and infrastructure including network devices, firewalls, load balancers, Network Access Control (NAC), and running the Network Operations Center (NOC).
People Team	Provides support for incidents involving policy violations by Teach For America employees and executes response activities regarding employees.
Risk and Compliance	Responsible for notifying insurance and maintaining communication with adjuster regarding the status of the incident. Provides regulatory compliance advice and consultation for all incidents with regulatory implications, enlists the assistance of other departments in the enforcement of these regulations during an incident. Responsible for external communications in coordination with the IR Coordinator, Communications Lead, Legal Affairs, and the Security Lead. Internal communications will be handled in conjunction with the IR Manager and Communications Lead.
Service Desk Platform	Provides technical support to the Core Team in relation to Teach For America user(s) inquiries during an incident and Incidents where user endpoints are directly involved. Escalates to Security Operations Analysts on suspicious events reported by users.
Web Platform	Provides technical support to the Core Team in relation to Teach For America's web presence and web stack.
Workload Management Platform	Provides technical support to the Core Team in relation to Teach For America Linux and windows infrastructure. Responsible for provisioning & managing computing workloads, virtualization, storage, data backup & recovery
Workplace Technology Services	Provides technical support to the Core Team in relation to Teach For America end user computing, including software imaging, endpoint policies, image for devices across the enterprise, Microsoft product licenses.

- *Third Parties*

Third parties are external to Teach For America but can also provide support to the Core Team when called upon. Their activities can vary from technical to management consultation support. The Security & Compliance Team and Office of General Counsel & Risk are responsible for initiating communications with them. The Third-Party Team can consist of the following entities:

Third Parties		
Role	**Responsibility**	**Owner**
Cyber Insurance Provider	Provides Teach For America with support per the current insurance agreement. The Risk and Compliance Team will initiate the communication process with the cyber insurance provider.	**Compliance Team**
Managed Detection & Response	Rapid7's MDR service rapidly detects, investigates, contains and eradicates threats in our environment, and is delivered as a collaboration between Rapid7 and our team. Rapid7 is a true extension of the security team by providing hands-on 24x7x365 monitoring, threat hunting, **incident response**, and customized security guidance to stop malicious activity and strengthen our security posture.	**t Compliance Team**
External Counsel	Provides legal support to the IR Team. The Risk and Compliance Team will initiate the communication process with external counsel. Note: The cyber insurance provider maintains a list of approved vendors. Historically, TFA has worked with Mullen Coughlin LLC.	**Compliance Team**
Law Enforcement	Supports Teach For America in handling criminal matters. The office of compliance will initiate the communication process with Police and other law enforcement entities.	**Legal Affairs**
Technology Vendors	Provides the Cybersecurity Incident Response Team with technical support for the tools utilized in the program. Support may be limited based on pre-existing agreements between Teach For America and its vendors. The IR Manager will facilitate communications between the Cybersecurity Incident Response Team and each technology vendor.	**blogy Point of Contact**
Credit Monitoring	Based on the type of breach (PII), TFA has legal notification requirements. TFA also provides those parties with 1 year of credit monitoring services through Experian.	**Compliance Team**

Incident Response Process

The Cybersecurity Incident Response Plan uses consistent processes in responding to all incidents. An escalation process runs concurrently with the operational process. The process consists of six major phases: Preparation, Detection, Containment, Eradication, Recovery, and Postmortem. Throughout these phases, response activities and observations will be continually documented, when applicable.

- Preparation

  The preparation phase is an ongoing process meant to implement the action items directed by previous incidents and lessons learned discussions. To optimize and improve the Cybersecurity Incident Response Plan, activities in this phase may include, but are not limited to:

- Training and skills development – The Core Team must continually develop its skills in order to maintain its technical proficiencies and familiarize itself with new threats.
- Incident simulations – Tabletops, Live War Game, and Purple Team exercises help identify gaps in the response process and practice the roles of both the Core and Extended Teams.
- Program metrics analysis – Performance analysis enables the Incident Response Team to track, measure, and identify areas of improvement for the CIRP.
- CIRP procedures refinement – Implementation of previously identified action items or new response procedures help enable an efficient response process.
- Detection capabilities enhancement – Improvements to existing technologies or implementing new monitoring tools can help aid with the detection of advanced threats.

- Detection

  The Detection Phase consists of activating a cybersecurity incident request, correlation, alert urgency/severity rating, and documentation of events being reported to the Security & Compliance Team, as well as validation of those alerts to incidents.

  After the event or alert has been identified, the event or alert is typically correlated through the different vectors to identify events that pose a potential threat to Teach For America. Once an event or alert is detected from various sources, the Security Operations Analyst performs an initial triage. Next The Security & Compliance Team may review with additional business units if the incident was reported by a business function outside of the Security & Compliance Team. Event or alert detection will include but not limited to:

- Microsoft Defender Suite:
  - Microsoft Defender for O365
  - Microsoft Defender for Endpoint
  - Microsoft Defender for Cloud Apps
- Rapid7 SIEM Insight IDR
- Extended Team Reported Event
- Third Party Reported Events
- User Reported Events

  Once validated, the Security Operations Analyst will need to complete the early triage form, open a Jira ticket titled “Security Incident”, and document all significant attributes, as well as classify the Incident Severity Rating and categorize the cybersecurity incident in the ticketing tool. The Security Operations Analyst notifies the Security & Compliance Team to prioritize the response process. The Security Operations Analyst should document, at a minimum, the following details in Jira ticket:

- Event times and dates
- Scope, including impacted assets (machine names and IP addresses)
- Classification, including incident category and severity rating
- Attack vector (if known)
- Impact description
- Indicators of compromise
- Task for extended team(s)

If the Incident Response Team has a reasonable basis to believe that a data breach of Teach For America confidential information has occurred, it must contact Risk & Compliance. Depending on the severity the CDTO and VPs of TDX may need to be contacted as well. Communications with Rapid7 Incident Response, law enforcement agencies, regulators, external counsel, the cyber insurer, and/or Leadership should be considered.

Incident Communications

Once an incident has been validated, the IR Manager will complete the following step and follow the notification guidelines below. Notifications will be sent by email if available, designated slack channel, and otherwise via out of band communications. The bridge dial-in information will be distributed by the IR Manager, when applicable.

- Start collaborating in the it_major_incident Slack channel.
  - Our practice is to maintain the conversation within the Slack thread.
- Create a Zoom meeting for major incident response team to participate. Post it to the it_major_incident Slack channel.
- Contact Rapid7 MDR Incident Response Team.
- Consolidate facts and assemble additional resources as needed, Production System Contact List.
- Communicate to the extended teams with technical details by using incident@ email distribution list. Provide regular updates until the incident has been resolved based on the table below.
- Provide a root cause analysis after the service is restored. An RCA template and an example are provided here.

The following table provides notification guidelines for incidents based on severity rating:

Severity Rating	IR Coordinator	Notification
High	· Assigned when incident confirmed	Within 2 hours of classification of an incident (Core team, Extended teams, and Senior Leadership team)
Medium	· IR Manager	Within 24 hours of classification of an incident (Core team and Relevelant Extended teams)
Low	· Security Operations Analyst(s)	Within 48 hours of classification of an incident (Core team only, Extended team if needed)

The table below provides guidelines for providing updates within the Incident Response Team and to leadership based on incident severity:

Severity Rating	Notification Lead	Initial notification requirements	On-going IR Team updates	On-going leadership updates
High	Communications Lead	Within 2 hours of classification of an incident	Every 4 hours until containment	Every 8 hours until containment
Medium	Security Analyst	Within 24 hours of classification of an incident	Every 24 hours until containment	N/A
Low	Security Analyst	Within 48 hours of classification of an incident	Weekly update	N/A

- Containment

Containment begins with input from the detection phase and may follow the incident through the response efforts. The goal of the containment phase is to effectively minimize the spread and impact of an identified incident within the Teach For America environment and limit the incident from spreading outside of Teach For America. Further damage may occur even though containment has taken place, as gaps in scope may still lead to further impact.

The Incident Response Team begins developing a containment strategy once all significant attributes have been documented. The containment strategy should include criteria of the business risk or impact of the containment strategy, additional business units to engage (as needed), and criteria for what constitutes successful containment. The IR Manager should then review the containment strategy with the Incident Response Team, and obtain the necessary approvals based on the containment strategy.
Once the threat has been successfully contained, the Incident Response Manager may de-escalate the incident to a lower severity rating at their discretion.

The Incident Response Manager coordinates with the appropriate Extended Team members to contain the threat. While the Incident Response Manager is accountable for the successful execution of the containment activities, such activities can be delegated to other resources within the Extended Team. The major actions that take place during this phase may include:

- Core Team and Extended Team execute the containment strategy actions (e.g. blocking network traffic at the perimeter, isolating affected devices from the network, disabling certain functionalities, issuing an enterprise-wide password reset, etc.).
- Based on available information, the Core Team may be able to determine the root cause, which can influence the containment strategy.
- Monitor for deviations from the expected result(s).
- Update documentation (e.g. Slack channel and Jira).

- Determine if the containment strategy is successful. If the containment strategy is unsuccessful, return to developing a strategy. The team may go through multiple iterations and strategies before containment is successful.
- Determine if remediation is complete; if it is, resolve the incident. If remediation is incomplete, continue to eradication.

- ### Eradication

  The eradication phase encompasses resolving incidents by removing the threat from the environment. The Core Team begins developing an eradication strategy after containment has been completed or in parallel with the containment phase and follows the incident until it has been successfully resolved. The Incident Response Team will obtain the necessary approvals from the Extended team based on the eradication strategy. Once the strategy has been developed, the Core Team should seek approval from the Extended Team prior to executing the eradication plan.

  While the Incident Response Manager is accountable for the successful execution of the eradication activities, they can be delegated to other resources within the Core Team and Extended Team. Once approved, the Core Team should execute the eradication actions. The tasks in this phase typically consist of removing the source of the threat and its associated entities. Activities for this phase can include, but are not limited to:

- Removing malware
- Deleting phishing emails
- Decommissioning a faulty device

  The Core Team must monitor the network closely following eradication for indications of the threat re-emerging. Following monitoring, the documentation (e.g. Slack Channel and incident management tool) should be updated. The IR Manager will then determine if the eradication strategy is successful. The Incident Response Manager will coordinate with the appropriate teams to perform alternative eradication plans, if the eradication strategy is unsuccessful.

  Once eradication actions are successful, the IR Manager will determine if remediation is complete. If remediation is not complete, the Core Team will proceed to the recovery phase. If remediation is complete, the incident should be resolved. The Incident Report should be updated and sent to the Incident Response Team when moving to the recovery phase. This task should be conducted even when out of normal frequency.

- ### Recovery

  The goal of the recovery phase is to determine the recoverability of affected assets and, when possible, return the assets to normal business operations. The Incident Response Manager and System/Product owner develops a recovery strategy after eradication has been completed and follows the incident until it has been successfully resolved. The Core and Extended Teams will then execute the recovery actions determined in the recovery strategy.

While the Incident Response Team is accountable for the successful execution of the recovery activities, they can be delegated to other resources within the Incident Response Team. Recovery activities for this phase can include, but are not limited to:

- Issuing new laptop to impacted user
- Rebuilding or reimaging affected devices
- Restoring data to affected devices
- Reconfiguring settings on affected devices
- Re-introducing a device into the production environment
- Monitoring for abnormal behaviors and verifying the continuation of normal business operations

The Core Team will monitor the recovery results for deviations from the expected outcome. Following monitoring, the documentation (e.g. Slack Channel and incident management tool) should be updated. The IR Manager will then determine if the recovery strategy is successful. The Incident Response Manager will coordinate with the appropriate teams to perform alternative eradication plans if the recovery strategy is unsuccessful.

Once it has been determined that remediation is completed, the Incident Response Manager will resolve the incident in the incident management tool. The Communications Lead will then inform the Incident Response Team that the incident has been resolved, signifying that operations have returned to normal, and send any final external communications based on the communication types.

- ### Postmortem

The Postmortem phase is used to identify improvement opportunities for the Cybersecurity Incident Response Plan and confirm that the feedback is documented and reported to the appropriate teams. Activities for this phase will be executed at the end of the Incident Response Process for all High incidents and select medium severity incidents. All documentation pertaining to the incident should be compiled. The incident documentation should be used to complete the full incident report. A post-mortem lessons learned meeting must be held no later than one week after the incident is fully remediated to identify improvement opportunities.

The meeting will assess the Response Process for gaps pertaining to the incident. These gaps will be translated into action items that can be used to improve the response process for future incidents.

Program Maintenance

- ### Training

Core Team members must have knowledge of cyber threats, threat mitigation, incident resolution, and investigations. In addition, Core Team personnel are further encouraged to specialize in related skill sets, such as computer forensics, malware reverse engineering, and threat intelligence gathering. All skills must be maintained and continually developed so the Core Team can enhance their skills and technical proficiencies for responding to incidents.

- Testing

  The Extended Team members must also maintain their skills. Since the team does not participate in incident response activities on a regular basis, an internal training program with the Core Team must be conducted to refresh the knowledge of program procedures and responsibilities for each role:

Exercise	Description
Tabletop	A facilitated discussion aimed at assessing the organization's response to a predetermined cyber-attack scenario. The exercise tests the functional elements of the IR Team with participation from the relevant business units. It is recommended that tabletop exercises be conducted on a quarterly basis.

Teach For America

Appendix

- **Contact Lists**

  - Production Systems Contact List
  - On-Call and Contact Info Confluence page
  - Single Source of Truth VM

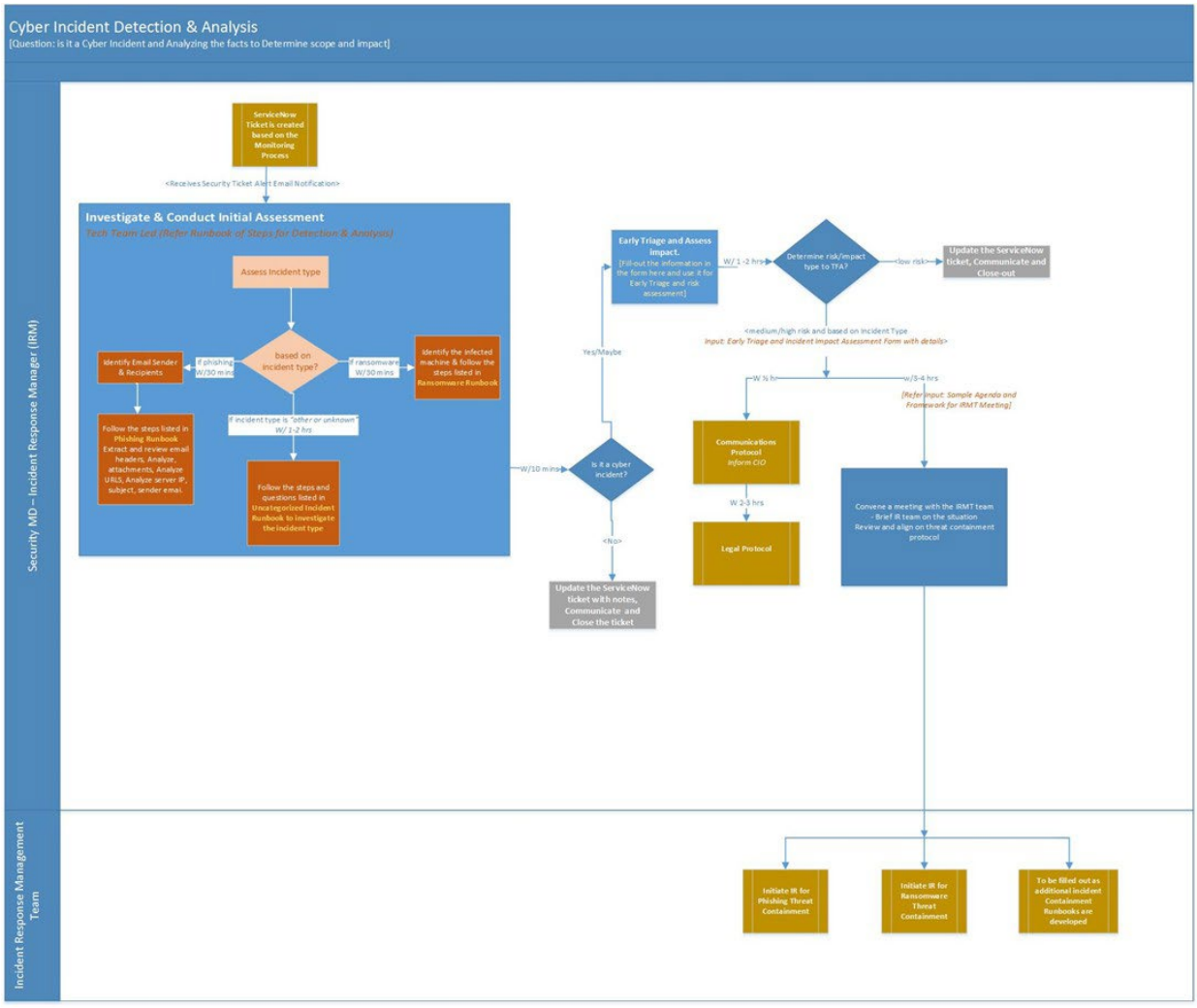
- Early Triage Impact Assessment
- Incident Response Report Template
- Root Cause Analysis Report Template

- **Agenda for IRT Call**

1. Assign a note-taker for purposes of disseminating action items and the status of responses.
2. Establish a regular communication schedule.
3. Legal to provide a privilege and confidentiality warning, and instructions for privileging communications.
4. Provide an update of facts.
5. Discuss and determine strategy — escalate immediately in a methodical process in the event of disagreement on strategy, *i.e.*, pulling production servers offline, public communications, reaching out to partners or law enforcement, etc.
6. Determine if other business units are needed and identify points of contact to support response/investigations.
7. Determine whether the IRT Executive Committee should be notified, and use established processes for informing the IRT Executive Committee as to the event and to provide regularly scheduled briefings/updates on the response/investigation. Identify who is responsible for such briefings, and the format of such briefings (*e.g.*, written, verbal, etc.).

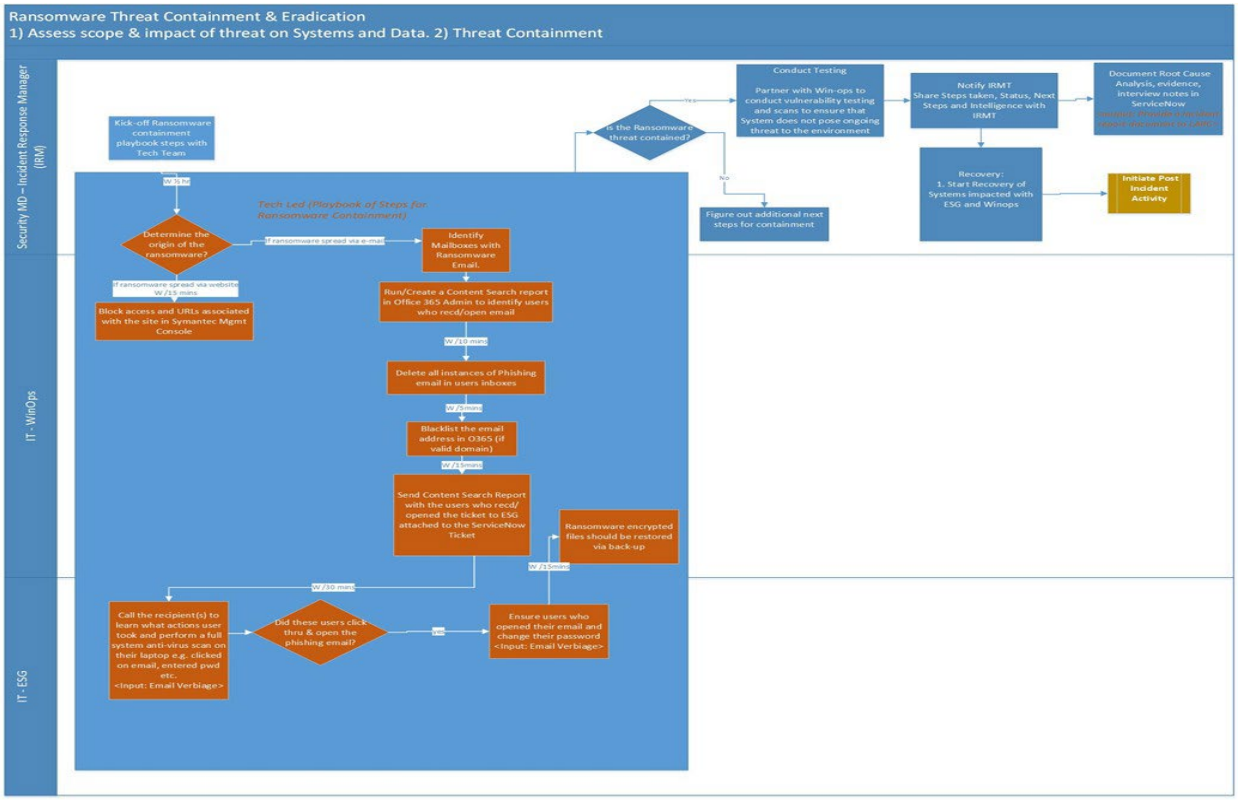
- **Process & Communication Workflow Examples**

High Level Workflow for Detection and Analysis Phase

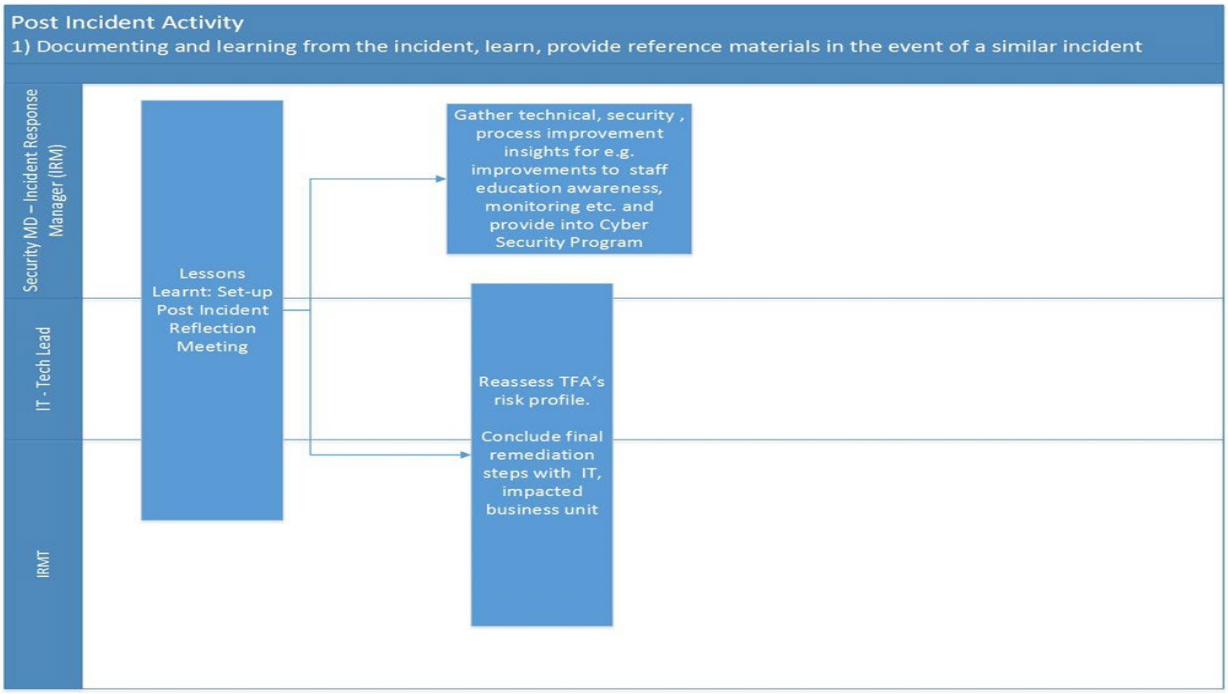


Teach For America

High Level Workflow for Ransomware Threat Containment and Eradication

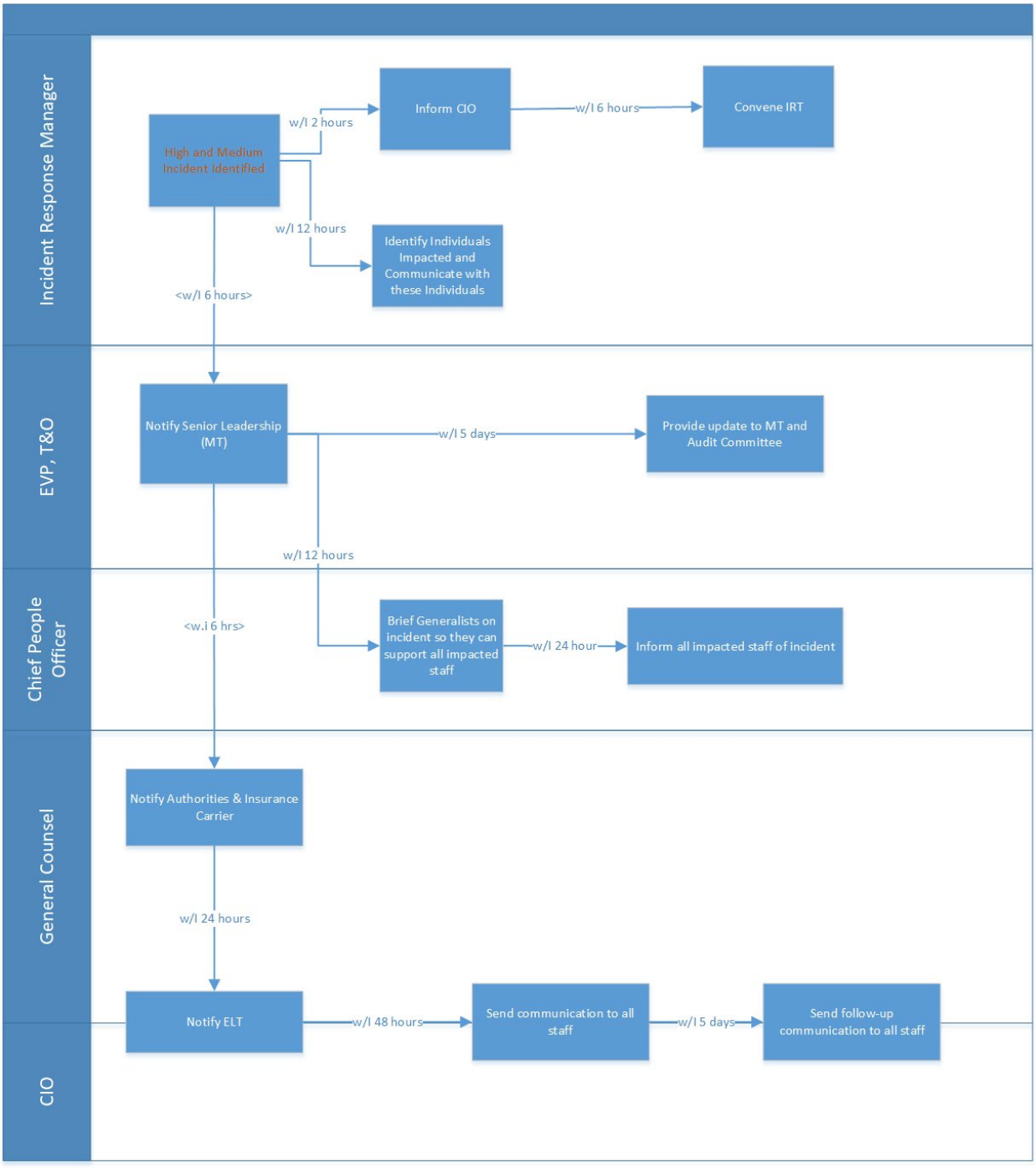


High Level Workflow for Post-Incident Activity



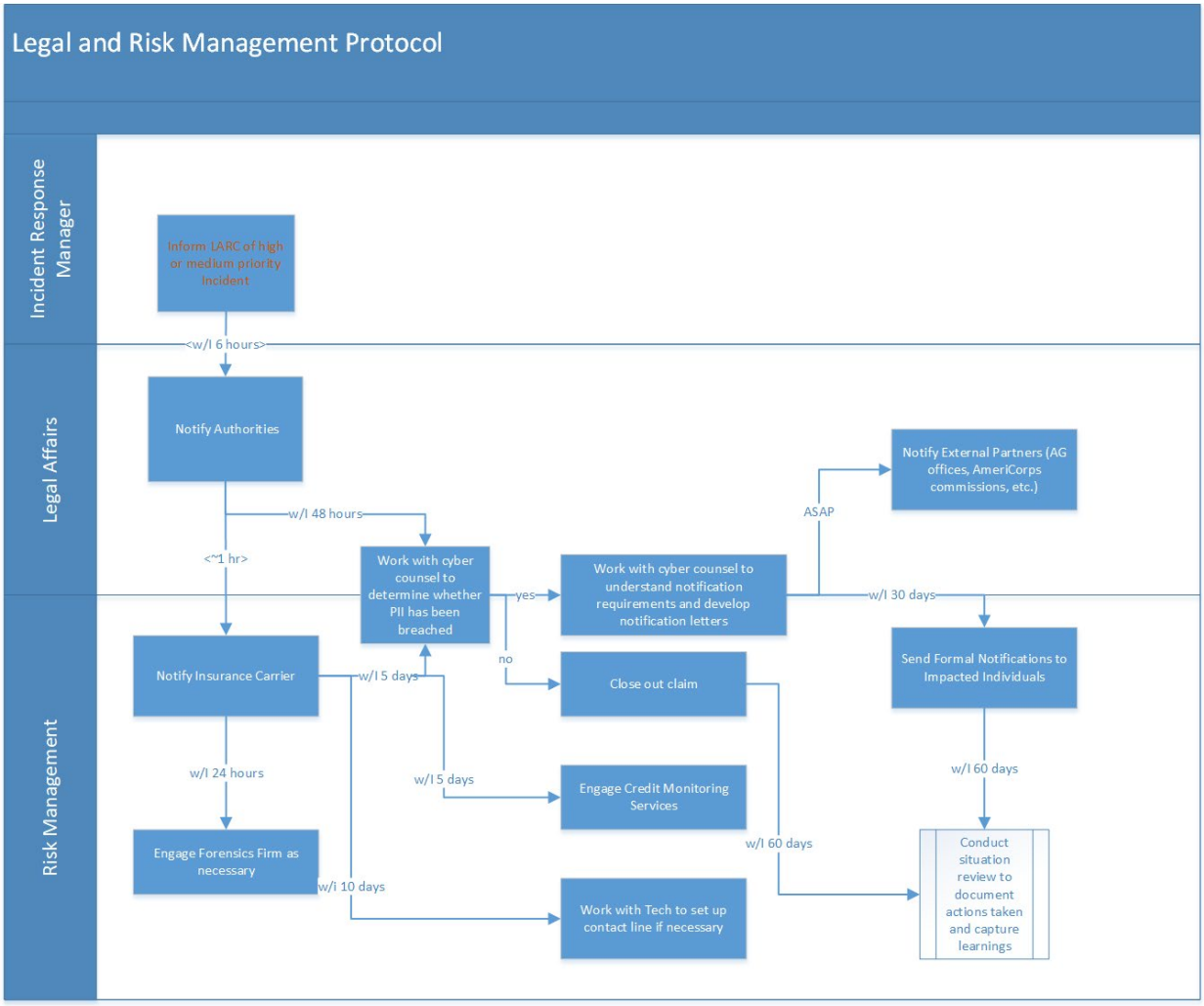
Teach For America

Communications Protocol



Teach For America

Legal and Risk Management Protocol



Teach For America

SCHEDULE E to Data Sharing Agreement

DESCRIPTION OF SYSTEM(S) USED IN THE TRANSFER OF PARTNER VIDEO & AUDIO DATA, FREQUENCY AND SECURITY FEATURES

System Description:
Video & Audio Storage Systems Description:

This **Schedule E** shall serve as Teach For America-San Antonio's official notification of the use of video and audio storage for corps member teacher coaching and training. Below we've outlined the various ways Teach For America- San Antonio and Participants will utilize the video and audio storage platform, including but not limited to:

- Uploading and reviewing classroom recordings and other content to engage in discourse and feedback on teaching practices.
- Foster strong dialogue and collaboration with other Participants and Teach For America staff as they share resources, ideas, and feedback.
- Streamline coaching conversations centered on individual teacher development, rooted in evidence from their classrooms, and use evidence-based practices modeled by other teachers.

As part of our use of classroom video and audio, Teach For America Participants will be uploading their classroom recordings. Although the video recordings are focused and framed around the teacher, there may be times they include student images.

Video and Audio Storage Security Features:
Although Participants will upload classroom recording videos and audio, these recordings are not sharable outside of the platform and only the corps member who uploaded the recording and Teach For America coaches have rights to download it. Data is encrypted in transfer as well as at rest when it is being stored in the data repository. We use a "least privilege granted" model for access to internal systems, employing multi-factor authentication where feasible, and monitor access across these systems with auditable logs.
Our video and audio storage platform meets rigorous data security and privacy standards as a closed and private platform and complies with laws and regulations concerning the privacy, security, and notification of breaches.