



**BILL HASLAM**  
GOVERNOR

STATE OF TENNESSEE  
**DEPARTMENT OF EDUCATION**  
NINTH FLOOR, ANDREW JOHNSON TOWER  
710 JAMES ROBERTSON PARKWAY  
NASHVILLE, TN 37243-0375

**CANDICE MCQUEEN**  
COMMISSIONER

FISCAL REVIEW COMMITTEE PACKET  
CONTRACT #: 56904  
TRACKING #:33132-00317  
VENDOR: Teachstone Training, LLC.

1. Summary Letter
2. Supplemental Documentation Form
3. Edison Query
4. Original Contract
5. Approved Amendment #1 Request Form
6. Amendment #1



**BILL HASLAM**  
GOVERNOR

STATE OF TENNESSEE  
**DEPARTMENT OF EDUCATION**  
NINTH FLOOR, ANDREW JOHNSON TOWER  
710 JAMES ROBERTSON PARKWAY  
NASHVILLE, TN 37243-0375

**CANDICE MCQUEEN**  
COMMISSIONER

TO: Executive Director, Fiscal Review Committee

FROM: Candice McQueen, Commissioner

DATE: May 15, 2018

RE: Request to appear before fiscal review committee regarding non-competitive contract amendment request RFS # 33132-00317

Please consider the enclosed request for a non-competitive contract amendment with Teachstone Training, LLC (Teachstone). Teachstone is currently delivering a pilot of data collection and professional development for voluntary pre-K (VPK) program quality monitoring in 200 classrooms, and the department of education is seeking an amendment to expand this work to all VPK and Preschool Development Grant (PDG) classrooms across the state. An amendment is needed to update the scope to reflect this expansion, increase the maximum liability to \$895,812.00, and update the payment methodology.

Under the Pre-K Quality Act of 2016, the department is required to work toward improving the consistency of quality in pre-K classrooms across the state. To accomplish this work, we must gather data regarding current program quality practices, as very little data currently exists on Tennessee pre-K programs. Teachstone's CLASS tool is an in-class rating system that rates the quality of practice by measuring student/teacher interactions. The rater observes the classroom over a period of four hours and takes samplings of interactions. This tool generates reports regarding those observations, which will be used to develop future professional development and supports for classrooms.

The CLASS tool is currently being used to gather baseline data regarding quality program standards in 200 VPK classrooms. Expanding the pilot to include data-gathering of all VPK and PDG classrooms is necessary to comprehensively assess classroom climate, organization, and instructional support statewide. This data will enable the department to meet its legal obligations under the Pre-K Quality Act to decrease the variability of quality in VPK and PDG classrooms and ensure high quality practices are being supported throughout the state.

Teachstone also provides on-site teacher trainings to provide an overview of the CLASS evaluation tool including what is measured, how it is measured, and how to change practice as a result of the measurements. The amendment will increase the number of teacher trainings in order to ensure that teachers are supported in this work.

Alternative procurement options are not available for this work, as Teachstone is the sole provider of the CLASS system, the only system that supplies analysis of teacher-student interactions in the pre-K classroom. As Teachstone collected data for the 200 pilot classrooms, the department must continue this work with Teachstone to maintain data validity with the remaining 789 VPK and PDG classrooms. Therefore, it is in the best interest of the State to amend this contract.

Thank you for your consideration.

Supplemental Documentation Required for  
Fiscal Review Committee

*Contact Name:	Joanna Collins	*Contact Phone:	615-770-3869
*Presenter's name(s):	Elizabeth Alves, Candace Cook, Jessica Lord, Joanna Collins, Elizabeth Fiveash		
Edison Contract Number: <i>(if applicable)</i>	56904	RFS Number: <i>(if applicable)</i>	33132-00317
*Original or Proposed Contract Begin Date:	1/19/2018	*Current or Proposed End Date:	1/18/2019
Current Request Amendment Number: <i>(if applicable)</i>	1		
Proposed Amendment Effective Date: <i>(if applicable)</i>	60 days from submission date		
*Department Submitting:	Department of Education		
*Division:	Early Learning and Literacy		
*Date Submitted:	5/14/2018		
*Submitted Within Sixty (60) days:	Yes		
<i>If not, explain:</i>	N/A		
*Contract Vendor Name:	Teachstone Training, LLC		
*Current or Proposed Maximum Liability:	\$895,812.00		
*Estimated Total Spend for Commodities:	N/A		
<b>*Current or Proposed Contract Allocation by Fiscal Year: (as Shown on Most Current Fully Executed Contract Summary Sheet)</b>			
FY: 2018	FY: 2019	FY:	FY:
\$190,850.00	\$704,962.00	\$	\$
<b>*Current Total Expenditures by Fiscal Year of Contract: (attach backup documentation from Edison)</b>			
FY:	FY: 2019	FY:	FY:
\$0.00	\$0.00	\$	\$
<b>IF</b> Contract Allocation has been greater than Contract Expenditures, please give the reasons and explain where surplus funds were spent:	The first 200 observations have been recently completed. The Contractor became eligible to invoice the State upon completion of these observations and the current invoice is in process.		
<b>IF</b> surplus funds have been carried forward, please give the reasons and provide the authority for the carry forward provision:			
<b>IF</b> Contract Expenditures exceeded Contract Allocation, please give the reasons and explain how funding was acquired to pay the overage:			

Supplemental Documentation Required for  
Fiscal Review Committee

<b>*Contract Funding Source/Amount:</b>			
State:	\$305,942.00	Federal:	\$589,870.00
<i>Interdepartmental:</i>		<i>Other:</i>	
If “ <i>other</i> ” please define:		N/A	
If “ <i>interdepartmental</i> ” please define:		N/A	
Dates of All Previous Amendments or Revisions: <i>(if applicable)</i>		Brief Description of Actions in Previous Amendments or Revisions: <i>(if applicable)</i>	
N/A		N/A	
Method of Original Award: <i>(if applicable)</i>		Sole source	
<p style="text-align: center;">*What were the projected costs of the service for the entire term of the contract prior to contract award? How was this cost determined?</p>		<p>The original projected costs for the contract were \$190,850.00. The cost was determined in accordance with standard pricing provided by the vendor and pricing they provide to other state education agencies. The original projected costs were limited to the initial pilot, as future funding and project expansion plans were unknown at that time.</p>	
<p style="text-align: center;">*List number of other potential vendors who could provide this good or service; efforts to identify other competitive procurement alternatives; and the reason(s) a sole-source contract is in the best interest of the State.</p>		<p>Alternative procurement options are not available for this work, as the contractor is the sole provider of the CLASS system, the only system that supplies analysis of teacher-student interactions in the pre-K classroom.</p>	

Payments against a Contract	0
-----------------------------	---

Unit	Sum Merchandise Amt	Edison Contract ID	Vendor ID	Vendor Name	Type
------	---------------------	--------------------	-----------	-------------	------

PO ID	Voucher ID	Invoice	Date	Fiscal Year
-------	------------	---------	------	-------------

 <b>CONTRACT</b> (fee-for-goods or services contract with an individual, business, non-profit, or governmental entity of another state)					
Begin Date January 19, 2018		End Date January 7, 2019		Agency Tracking # 33132-00317	Edison Record ID
Contractor Legal Entity Name Teachstone Training, LLC					Edison Vendor ID 0000206628
Goods or Services Caption (one line only) Voluntary Pre-K Program Quality Monitoring and Professional Development					
Contractor <input checked="" type="checkbox"/> Contractor			CFDA # N/A		
Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2018	\$190,850.00				\$190,850.00
<b>TOTAL:</b>	\$190,850.00				\$190,850.00
<b>Contractor Ownership Characteristics:</b> <input type="checkbox"/> Minority Business Enterprise (MBE): African American, Asian American, Hispanic American, Native American <input type="checkbox"/> Woman Business Enterprise (WBE) <input type="checkbox"/> Tennessee Service Disabled Veteran Enterprise (SDVBE) <input type="checkbox"/> Tennessee Small Business Enterprise (SBE): \$10,000,000.00 averaged over a three (3) year period or employs no more than ninety-nine (99) employees. <input checked="" type="checkbox"/> Other: N/A					
<b>Selection Method &amp; Process Summary</b> (mark the correct response to confirm the associated summary)					
<input type="checkbox"/> Competitive Selection			Describe the competitive selection process used		
<input checked="" type="checkbox"/> Other			Sole Source procurement via approved special contract request - the contractor is the sole provider of the CLASS system, the only system that supplies analysis of teacher-student interactions in the pre-K classroom.		
<b>Budget Officer Confirmation:</b> There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.					
 Digitally signed by Chris Foley DN: cn=Chris Foley, o=Tenn Dept of Education, ou=OCFO, email=chris.foley@tn.gov, c=US Date: 2018.01.04 09:51:22 -06'00'					
Speed Chart (optional) ED1205			Account Code (optional) 911402		

**CONTRACT  
BETWEEN THE STATE OF TENNESSEE,  
DEPARTMENT OF EDUCATION  
AND  
TEACHSTONE LLC.**

This Contract, by and between the State of Tennessee, Department of Education ("State") and Teachstone Training, LLC ("Contractor"), is for the provision of Voluntary Pre-K program quality monitoring and professional development, as further defined in the "SCOPE." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is a Limited Liability Company.

Contractor Place of Incorporation or Organization: Charlottesville, Virginia

Contractor Edison Registration ID # 0000206628

**A. SCOPE:**

- A.1. The Contractor shall provide all goods or services and deliverables as required, described, and detailed below and shall meet all service and delivery timelines as specified by this Contract.
- A.2. Definitions:
- a. CLASS evaluation system – a rating scale, reporting system and online tools through which preschool (Pre-K) classrooms are evaluated and outcomes are reported.
  - b. Materials - any products, printed, or electronic versions that the Contractor owns or uses in the process of delivering services to the State.
  - c. myTeachStone – the Contractor's online data collection system that is aligned with professional development and coaching
  - d. Office of Early Learning (OEL) – The Tennessee Department of Education state office governing early childhood programs quality and compliance
  - e. Pilot Participant – 200 VPK classrooms being evaluated pursuant to this Contract, selected randomly by the State.
  - f. Train the Trainer (TTT) – Training for staff within the department of education that will prepare staff to lead trainings on use of the CLASS evaluation system to educators in the state
  - g. Voluntary Pre-K (VPK) – All state funded pre-k classrooms as defined in the Voluntary Pre-K for Tennessee Act of 2005, Tenn. Code Annotated Title 49, Chapter 6, Part 1.
- A.3. Using the CLASS evaluation system, the Contractor shall conduct in-person observations of student/teacher interactions in 200 Tennessee Voluntary Pre-K (VPK) classrooms, designated by OEL, and provide feedback and reports to the State. This shall include at minimum:
- a. Observations shall have a specific focus on emotional support, classroom organization and instructional support, and all of their subcategories as listed in the CLASS Dimensions Guide.
  - b. The Contractor shall complete 1 four cycle observation of each classroom within the first 90 days of the Contract. For these purposes, a four cycle observation takes place over a two hour time period (consisting of four thirty (30) minute cycles) and includes snapshots of interactions at four different points during that period.
  - c. The Contractor shall provide data reports to the State in the myTeachstone system including the in-person rating of the classroom quality using the CLASS evaluation system. Data reports shall include classroom, school, district, and State level data and not contain student personally identifiable information. The State shall have access to every Pilot Participant's data. The Contractor shall also provide a final report to the State that includes all raw data collected pursuant to this Contract.
  - d. If requested by the State, the Contractor shall provide reports on student-teacher interactions, as rated during the classroom observations, to OEL, school administrators and district coaches. Reports shall include all metrics evaluated by the CLASS evaluation system. School administrators and district coaches shall have access to

- feedback and reports related to their own classrooms, schools, and districts and will not have access to other Pilot Participants' data.
- e. All data gathered by the Contractor shall not be shared with third parties (including districts, teachers, and coaches) unless approved by the State. This pre-approval requirement also applies to providing districts with individual reports regarding teacher performance.
- A.4. If requested by the State, the Contractor shall provide initial observer training to no less than 2 members of OEL staff (could be additional attendees). Initial observer trainees will be trained to use the CLASS evaluation system with reliability.
  - A.5. Once staff are trained to observe, the Contractor shall provide TTT observer training to no less than 2 members OEL staff (could be additional attendees) within the first 6 months of the Contract. The TTT observer training covers training others to use the CLASS evaluation system and its rating scales and data analysis. TTT Trainees may subsequently train an unlimited number of State employees and a maximum of fifteen (15) district level observers during the term of this Contract. There is no limit on the number of Introduction to CLASS trainings that TTT Trainees may conduct.
    - a. The Contractor shall provide all Materials associated with TTT training, including: Participant guides for the Intro and Obs training, Facilitator guides for the Intro and Obs training, DVD/or flash drive of videos, participant guide for the TTT session, one dimension guide, one score sheet, an exemplar video description booklet, one year access to the Pre-K video library, (when completing training) access to the Affiliate Trainer Panel (this is where the powerpoints and other affiliate resources are), and a master code justification. The printed Materials should come in a big binder with tabs. One copy of the TTT training Materials shall be provided for each attendee.
  - A.6. If requested by the State, the Contractor shall provide up to 200 subscriptions for coaches, school administrators, OEL staff and classroom teachers to access myTeachstone, including all online training modules.
  - A.7. If requested by the State, the Contractor shall provide districts with access to use and receive training on the coaching companion tool within MyTeachstone, which contains training and resources. Access includes on-site training for up to 21 leaders and 5 OEL staff regarding use of coaching companion tool and how to differentiate professional development for teachers.
  - A.8. If requested by the state, the contractor shall provide up to 10 monthly one hour support calls or webinars with a coaching specialist for district leaders and/or coaches participating in the project. The Contractor shall make all arrangements with district leaders and/or coaches for the support calls or webinars. Teachstone will provide a schedule as to when calls will take place each month; this schedule will be provided at the beginning of the Contract term.
  - A.9. If requested by the State, the Contractor shall provide 4 on-site, full-day trainings for up to 50 teachers participating in the Pilot. These trainings will provide an overview of the CLASS evaluation tool including what is measured, how it is measured, and how to change practice as a result of the measurements.
    - a. If requested by the State, the Contractor shall provide copies of Materials so that the State trainers can conduct the trainings in-house. Materials include the CLASS Dimensions Guide and associated Materials.
  - A.10. If requested by the State, the Contractor shall provide 2 day observer training to district coaches (up to 15 participants). This will be a 2 day training that will provide participants with explicit instruction regarding the full content, scope and measures of the CLASS evaluation tool. Participants will be trained to use the tools to reliably observe classrooms using the tool. Participants will also be instructed on appropriate classroom practice in regard to student/ teacher interactions and emotional supports. All participants will receive a dimensions guide.

- A.11. The State shall have a limited, nontransferable, nonexclusive, and royalty-free right and license to use Materials provided to the State pursuant to this Contract term. The State acknowledges that Contractor is the owner of the Materials and all its contents.
- A.12. If the Contractor will have direct access to school children or children will be present when services are performed, the Contractor shall perform services only when school officials or employees are present and where the activity, assembly, or event is conducted under the supervision of school officials or employees, in accordance with the background check requirements in Tenn. Code Annotated § 49-5-413.
- A.13. Technical Requirements.

This section defines the technical requirements of the State for the Software as a Service (SaaS) product offering described in A.3 thru A.12.

a. Fault Tolerance

- i. The Contractor shall deliver an end to end solution, inclusive of the State software if applicable, server and architectural components that are fault tolerant and thoroughly tested at a scale commensurate with anticipated usage and volume under this Contract.
- ii. The solution shall recover from the following circumstances without a material degradation of the user experience and with minimal loss of end-user data:
  1. Brief loss of connectivity between the user and the Contractor's data center servers.
  2. Brief device non-responsiveness due to CPU bind, operating system activity or other local resource contention.
  3. Any message trapped and thrown by the Contractor's application software.
  4. Any event that occurs server-side in the Contractor's infrastructure related to load, concurrency, normal transients, or scheduled and unscheduled processes initiated by the Contractor.
- iii. The online solution shall be able to recover user state (status of user activity inside the application) for critical workflows once the application is available with or without end-user intervention under the following circumstances:
  1. The State device becomes permanently non-responsive for any reason.
  2. Malfunction or failure of the State device, including; battery depletion or loss of power on the State device.
  3. Log out or user error on the State device.
  4. Permanent loss of local area network, wide area network or internet connectivity between the State device and the Contractor's data center.
  5. Infrastructure failure at the State location.
  6. Application, browser or operating system "crash" or unexpected restart on local device.
  7. Unexpected failure or unavailability of a required resource at the Contractor's data center.

b. Data Persistence

- i. The Contractor shall develop database and data persistence strategies that are consistent with the scalability, performance, security and redundancy profile of an enterprise grade solution.
- ii. All data shall be stored, retained and exposed in a manner that is consistent with the requirements of the Federal Educational Rights and Privacy Act ("FERPA"), and other federal and state laws and policies as referenced in this Contract.

- iii. All data captured, manipulated, processed or transformed under this Contract remains the exclusive property of the State and may not be viewed, modified or disclosed to any party without the written approval of the State except for reasonable dealings as needed to execute on the deliverables of this Contract. Teachstone retains the right to use an anonymized, aggregated form of data to use in research and validity of its products, subject to FERPA.
- iv. Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State.

c. Data Transmission

- i. The Contractor agrees to work with the State to ensure bi-directional electronic data flows as needed to ensure that business application functionalities between the State and Contractor are efficient, secure and robust.
- ii. Working with the State is defined as;
  - 1. Reaching agreement on the schema of data structures for each data flow required.
  - 2. Reaching agreement on the protocol and format for the transmission of data in the most compatible way for all data consumers.
  - 3. Reaching agreement on the methodology and process for the efficient transmission of data.
  - 4. Reaching agreement on the security and authentication model for the most secure and trustworthy transmission of data.

d. District Infrastructure

- i. The Contractor is advised that school districts in Tennessee do not implement a standardized IT infrastructure statewide and as such multiple device makes and models, browser and operating systems exist. The Contractor shall deliver an online solution that is compatible with the matrix of devices and operating systems in use in the state and ensure that there is an equal fidelity of user experience regardless of the device or operating system in use. The Contractor shall deliver an online solution that ensures a high-quality user experience in current versions of standard web browsers, including Internet Explorer, Safari, Chrome, and Fire Fox.
- ii. The Contractor is advised that while all school districts in Tennessee are required to have high speed internet available to all locations within the district, the quality and performance of internet connectivity will vary considerably between districts due to factors such as; geography, infrastructure availability, specific carrier and QoS. The Contractor shall design and implement an online solution that functions in a predictable and usable manner across the range of connection speeds available in Tennessee.
- iii. The Contractor is advised that while all school districts in Tennessee are required to have sufficient wired and or wireless networking to ensure connectivity of student devices to the Internet, the quality and performance of local area networks will vary considerably between locations due to factors such as: equipment type, age of equipment, building construction and environmental factors. The Contractor shall design and implement an online solution that functions in a predictable and usable manner across the range of local area network speeds available in Tennessee.
- iv. The State shall provide the contractor with an up-to-date table of all specific district capabilities referred in this section at the start of the Contract.

e. Service Availability

- i. The Contractor shall implement systems and processes to ensure the availability of the online solution occurs in a manner consistent with service level agreements associated with this service.
- ii. Service availability requirements shall include but are not limited to:
  1. Scheduled maintenance and service outage notification protocols.
  2. An incident response team.
  3. Redundancy of broadband services into Contractor's data center.
  4. Redundancy of critical servers and other data center infrastructure.
  5. Active failover between redundant components.
  6. Backup power generation.
  7. Proactive monitoring and for service limiting exploits such as; Denial of Service (DoS) attacks.
  8. Following implementation, the System shall be available continuously, as measured over the course of each calendar month, an average of 99.9% of the time during Core business hours of 7:00 a.m. – 5:00 p.m. (CT) Mondays through Fridays, excluding State holidays. "Available" means the System shall be available for access and use by the State to conduct normal business associated with this system. For purposes of calculating the Availability Percentage, the following are "Exceptions" to the service level requirement and the System shall not be considered un-Available if any inaccessibility is due to:
    - a. customer-impacting downtime (which shall occur only upon advance written notice during non-core business hours); or
    - b. loss of the State's Internet connectivity
- iii. The Contractor shall provide to the State documentation outlining its Disaster Recovery Plan and Capabilities for said systems with contact information included in the event a DR event is executed.
  1. "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:
    - a. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: 2-4 hours
    - b. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: 8-12 hours
  2. The Contractor shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recover Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

f. Scalability

- i. The Contractor shall implement an infrastructure that has the ability to scale in a manner consistent with the volume, size and scale of expected usage under this Contract without service degradation or negative impact to active users.
  - ii. Scalability requirements shall include, but are not limited to:
    1. Broadband into the Contractor's data center takes into account the performance of peerage between the Contractors' broadband vendor and carriers in use in Tennessee school districts.
    2. Filtering and edge devices in the Contractor's data center.
    3. Local area networking within the Contractor's data center.
    4. Front end web servers.
    5. Caching and CDN.
    6. Middle tier servers including asynchronous and batch processing processes.
    7. Data access tiers and data throughput.
    8. Database storage.
    9. Data backup.
- g. Performance
- i. The Contractor shall provide a learning management system that is responsive to user interactions without a maximum wait time of 15 minutes.
  - ii. The Contractor shall ensure that where wait times are an expected part of the user experience, such as; loading a resource, the user receives a clear and unambiguous indicator that a long running action is taking place.
- h. Security
- i. The Contractor shall implement an online solution that is inherently secure and closely aligned with the rigorous data privacy standards of state and federal requirements, including FERPA.
  - ii. The Contractor must comply with the State's Enterprise Information Security Policies attached to this Contract as Attachment B.
  - iii. Security requirements shall include, but are not limited to:
    1. Encryption at rest for any data that includes personally identifiable information (PII) or FERPA protected information using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.
    2. Encryption in motion using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies, including use of a Transport Layer Security (TLS) 1.1 or higher encryption protocol between the State devices and the production servers.
    3. Data center certifications to ISO27001, SOC2 Type 2 or FEDRAMP standards: The Contractor shall provide proof of current certifications annually for itself and/or any partner organization who provides data center services in connection with this contract. The Contractor shall be responsible for ensuring that required data center certifications for itself and/or any partner organization remain current throughout the duration of this Contract.
    4. Access logging and intruder detection processes.
    5. Threat monitoring and vulnerability assessments, including; malicious exploits, such as; Man in the Middle and SQL Injection risk assessments.
    6. Data disposition process.
    7. Employee and Contractor vetting, and access control processes.
    8. User authentication processes.

9. Role management and user authorization processes.
10. Penetration testing as described in A.10.m.
11. All service housing personally identifiable Tennessee student information must reside in a data center located inside the United States.
12. Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

i. Capacity Planning

- i. The Contractor shall conduct capacity planning prior to commencement of service or service uplift to model demand and predict utilization across all components of the solution so that any potential deficiencies, resource constraints or capacity shortfalls can be identified and addressed prior to the commencement of the phase.
- ii. Capacity planning shall include, but is not limited to;
  1. Broadband capacity into the Contractor's data center takes into account the performance of peerage between the Contractors' broadband vendor and carriers in use in Tennessee school districts.
  2. Filtering and edge device capacity in the Contractor's data center.
  3. Local area networking capacity within the Contractor's data center.
  4. Front end web server capacity.
  5. Caching and CDN capacity.
  6. Middle tier server capacity including asynchronous and batch processing processes.
  7. Data access tiers and data throughput capacity.
  8. Database storage capacity.
  9. Data backup capacity.

j. Monitoring and Diagnostics

- i. The Contractor shall implement proactive exception alerting, real time monitoring and diagnostic capabilities for all components of the online solution.
- ii. Monitoring and diagnostics shall include, but is not limited to:
  1. Logging of user access events.
  2. Logging of key user interaction events to support an audit trail if needed.
  3. Detailed logging of application errors and anomalies with stack and trace data to support diagnostics in the event of problems.
  4. Logging of all system and server-side errors and anomalies.
  5. Real time "health" monitoring of all key servers and compute resources.
  6. Proactive exception monitoring of all key servers and compute resources based on thresholds and key performance indicators with escalating exception notifications.
  7. Implementation of inline performance counters and other common diagnostic "hooks" in key application source code.

k. Software Development Lifecycle

- i. The Contractor shall implement a methodical and structured software development lifecycle (SDLC) to minimize operational errors, improve transparency, drive inclusive decision making and ensure optimal quality assurance.
- ii. Development of an appropriate SDLC includes, but is not limited to:

1. An appropriate environment strategy for all software development to clearly delineate software that is in production versus that which is under development.
2. A rigorous change management policy to ensure the sanctity of the production environment and to minimize operational errors at critical times.
3. Inclusive process to notify the State Agency of activities potentially impacting student experiences, including; infrastructure upgrades, rolling new code, functional enhancements or changes to existing systems.
4. Robust quality assurance processes, including; code check-in rigor, usability testing, functional testing, scale and performance testing, code coverage testing and user acceptance testing.
5. Comprehensive bug lifecycle management.

#### I. Penetration Testing

- i. The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Penetration Tests" shall be in the form of software attacks on the Contractor's computer system, with the purpose of discovering security weaknesses, and potentially gaining access to the computer's features and data. The "Vulnerability Assessment" shall have the goal of defining, identifying, and classifying the security holes (vulnerabilities) in the Contractor's computer, network, or communications infrastructure. The Contractor will share the results of internal penetration testing with the State at the beginning of the Contract term and once per year after that while this Contract is in effect.
- ii. Penetration testing will be conducted against all public endpoints associated with the website providing the service.
- iii. With advance notice from the State, and no more than one (1) time per year the Contractor agrees to cooperate with the State to enable the State to request logical and physical audits of the Contractor's facility and systems that are hosting State data.

#### m. Accessibility

- i. The Contractor shall implement accessibility features for all users that follow Section 508 Standards and ADA compliance which requires the federal government to ensure that the electronic and information technology that it develops, procures, maintains, or uses is accessible to persons with disabilities.
- ii. Any updates to this standard will be the responsibility of the Contractor to plan, develop, test and deliver any mandated changes regarding these standards.

#### n. Compatibility

- i. In the event that the operating system is an integral part of the application, the Contractor agrees to maintain Operating Systems at current, manufacturer supported versions. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
- ii. The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. The Contractor shall make sure that the Application is at all times fully compatible with a manufacturer-supported Operating System; the

State shall not be required to run an Operating System that is no longer supported by the manufacturer.

- iii. If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application, to ensure that security vulnerabilities are not introduced.

- A.11. Warranty. Contractor represents and warrants that the term of the warranty ("Warranty Period") shall be the greater of the Term of this Contract or any other warranty general offered by Contractor, its suppliers, or manufacturers to customers of its goods or services. The goods or services provided under this Contract shall conform to the terms and conditions of this Contract throughout the Warranty Period. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge.

Contractor represents and warrants that the State is authorized to possess and use all equipment, materials, software, and deliverables provided under this Contract.

Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor's industry.

If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services. Any exercise of the State's rights under this Section shall not prejudice the State's rights to seek any other remedies available under this Contract or applicable law.

- A.12. Inspection and Acceptance. The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

*WJCM*  
B. **TERM OF CONTRACT:**

*15 CM*  
*19*  
*January 18, 2019* This Contract shall be effective for the period beginning on January 8, 2018 ("Effective Date") and ending on December 31, 2018 ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

- WJCM*  
B.1. Renewal Options. ~~This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to two (2) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.~~

- B.2. Term Extension. The State may extend the Term an additional period of time, not to exceed one hundred-eighty (180) days beyond the expiration date of this Contract, under the same terms and conditions, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.

C. **PAYMENT TERMS AND CONDITIONS:**

- C.1. **Maximum Liability.** In no event shall the maximum liability of the State under this Contract exceed one hundred ninety thousand, eight hundred and fifty dollars and zero cents (\$190,850) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.
- C.2. **Compensation Firm.** The payment methodology in Section C.3. of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor.
- C.3. **Payment Methodology.** The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.
- a. The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.
  - b. The Contractor shall be compensated based upon the following payment methodology:

Goods or Services Description	Amount (per compensable increment)
A.3. Live observation of up to 200 classrooms and provision of feedback and reports	\$100,000 total (\$500 per four cycle CLASS observation classroom evaluation)
A.4. Initial observer training for OEL staff	\$900 per staff member that receives training
A.5. TTT training for no less than two members of OEL staff, including all Materials	\$4,700 per staff member that receives training
A.6. up to 200 subscriptions to myTeachstone	Up to \$22,000 total (\$110 per subscription – per subscription cost includes start-up fee)
A.7. On-site training for 21 leaders and 5 OEL staff Coaching with myTeachstone. This is a 2 day (16 hour) training session.	Up to \$12,500 total; \$8,500 for the first 15 participants and \$350 for each additional participant.
A.8. Monthly support calls or webinars with coaching specialist, up to 10 calls	\$150 per call
A.9. Completion of 1 day (8 hour) on-site introduction to CLASS tool, for teachers (50 members)	\$7,000 per session
A.9(a). Materials for State trainers to provide training in-house	\$75 per copy of materials
A.10. CLASS observation training, two 2 day (16 hour) sessions, including Materials	\$8,500 per session.

- C.4. **Travel Compensation.** The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.
- C.5. **Invoice Requirements.** The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3., above. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have

been provided to the following address:

Tennessee Department of Education  
 Department of Early Learning  
 710 James Robertson Parkway, 11<sup>th</sup> floor  
 Nashville, TN 37243

- a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):
- (1) Invoice number (assigned by the Contractor);
  - (2) Invoice date;
  - (3) Contract number (assigned by the State);
  - (4) Customer account name: Tennessee Department of Education, Division of Early Learning and Literacy, Office of Early Learning
  - (5) Customer account number (assigned by the Contractor to the above-referenced Customer);
  - (6) Contractor name;
  - (7) Contractor Tennessee Edison registration ID number;
  - (8) Contractor contact for invoice questions (name, phone, or email);
  - (9) Contractor remittance address;
  - (10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
  - (11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
  - (12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
  - (13) Amount due for each compensable unit of good or service; and
  - (14) Total amount due for the invoice period.
- b. Contractor's invoices shall:
- (1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;
  - (2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
  - (3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
  - (4) Include shipping or delivery charges only as authorized in this Contract.
- c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

- C.6. Payment of Invoice. A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.
- C.7. Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.
- C.8. Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

- C.9. Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.
- a. The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and
  - b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

**D. MANDATORY TERMS AND CONDITIONS:**

- D.1. Required Approvals. The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.
- D.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State:

Candace Cook, Voluntary Pre-K Director  
 Tennessee Department of Education  
 Department of Early Learning  
 710 James Robertson Parkway, 11<sup>th</sup> floor  
 Nashville, TN 37243  
 Candace.Cook@tn.gov  
 Telephone # (615)741-9051  
 FAX # (615) 532-5303

The Contractor:

Sedra Spano, Regional Director  
 Teachstone Training LLC  
 675 Peter Jefferson Parkway, Suite 400, Charlottesville, VA 22911

Sedra.spano@teachstone.com  
 Telephone # ~~434.998.3909~~ 704.641.6802  
 FAX # 434.227.5434



All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

- D.3. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials.

- D.4. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.
- D.5. Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.
- D.6. Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to immediately terminate the Contract and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity for breach of this Contract.
- D.7. Assignment and Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.
- D.8. Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.
- The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.
- D.9. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.
- D.10. Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the

state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

- a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment A, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.
  - b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.
  - c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.
  - d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.
  - e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.
- D.11. Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.
- D.12. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.
- D.13. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.
- D.14. Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.
- D.15. Independent Contractor. The Parties shall not act as employees, partners, joint venturers, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party

to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.

- D.16. Patient Protection and Affordable Care Act. The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.
- D.17. Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, money, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.
- D.18. Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.
- D.19. Hold Harmless. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys for the State to enforce the terms of this Contract.

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

- D.20. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.
- a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.
  - b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.

- c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.
  - d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.
- D.21. Tennessee Consolidated Retirement System. Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq.*, the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.
- D.22. Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.
- D.23. Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:
- a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;
  - b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;
  - c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and
  - d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.
- The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded, disqualified, or presently fall under any of the prohibitions of sections a-d.
- D.24. Force Majeure. "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar

cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.

- D.25. State and Federal Compliance. The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract.
- D.26. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.
- D.27. Entire Agreement. This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.
- D.28. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.
- D.29. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.
- D.30. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:
- a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;
  - b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes [identify attachments and exhibits];
  - c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;
  - d. the State solicitation, as may be amended, requesting responses in competition for this Contract;
  - e. any technical specifications provided to proposers during the procurement process to award this Contract; and

f. the Contractor's response seeking this Contract.

- D.31. Iran Divestment Act. The requirements of Tenn. Code Ann. § 12-12-101 et.seq., addressing contracting with persons as defined at T.C.A. §12-12-103(5) that engage in investment activities in Iran, shall be a material provision of this Contract. The Contractor certifies, under penalty of perjury, that to the best of its knowledge and belief that it is not on the list created pursuant to Tenn. Code Ann. § 12-12-106.
- D.32. Insurance. Contractor shall maintain insurance coverage as specified in this Section. The State reserves the right to amend or require additional insurance coverage, coverage amounts, and endorsements required under this Contract. Contractor's failure to maintain or submit evidence of insurance coverage, as required, is a material breach of this Contract. If Contractor loses insurance coverage, fails to renew coverage, or for any reason becomes uninsured during the Term, Contractor shall immediately notify the State. All insurance companies providing coverage must be: (a) acceptable to the State; (b) authorized by the Tennessee Department of Commerce and Insurance ("TDCI"); and (c) rated A- / VII or better by A.M. Best. All coverage must be on a primary basis and noncontributory with any other insurance or self-insurance carried by the State. Contractor agrees to name the State as an additional insured on any insurance policy with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) insurance. All policies must contain an endorsement for a waiver of subrogation in favor of the State. Any deductible over fifty thousand dollars (\$50,000) must be approved by the State. The deductible and any premiums are the Contractor's sole responsibility. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements.

To achieve the required coverage amounts, a combination of an otherwise deficient specific policy and an umbrella policy with an aggregate meeting or exceeding the required coverage amounts is acceptable. For example: If the required policy limit under this Contract is for two million dollars (\$2,000,000) in coverage, acceptable coverage would include a specific policy covering one million dollars (\$1,000,000) combined with an umbrella policy for an additional one million dollars (\$1,000,000). If the deficient underlying policy is for a coverage area without aggregate limits (generally Automobile Liability and Employers' Liability Accident), Contractor shall provide a copy of the umbrella insurance policy documents to ensure that no aggregate limit applies to the umbrella policy for that coverage area.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified in this Section. The COI must be on a form approved by the TDCI (standard ACORD form preferred). The COI must list each insurer's National Association of Insurance Commissioners (NAIC) number and be signed by an authorized representative of the insurer. The COI must list the State of Tennessee – CPO Risk Manager, 312 Rosa L. Parks Ave., 3<sup>rd</sup> floor Central Procurement Office, Nashville, TN 37243 as the certificate holder. Contractor shall provide the COI ten (10) business days prior to the Effective Date and again thirty (30) calendar days before renewal or replacement of coverage. Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that subcontractors are included under the Contractor's policy. At any time, the State may require Contractor to provide a valid COI. The parties agree that failure to provide evidence of insurance coverage as required is a material breach of this Contract. If Contractor self-insures, then a COI will not be required to prove coverage. Instead Contractor shall provide a certificate of self-insurance or a letter, on Contractor's letterhead, detailing its coverage, policy amounts, and proof of funds to reasonably cover such expenses.

The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent

the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

**The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.**

a. Commercial General Liability Insurance

- 1) The Contractor shall maintain commercial general liability insurance, which shall be written on an Insurance Services Office, Inc. (also known as ISO) occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises/operations, independent contractors, contractual liability, completed operations/products, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).

The Contractor shall maintain bodily injury/property damage with a combined single limit not less than one million dollars (\$1,000,000) per occurrence and two million dollars (\$2,000,000) aggregate for bodily injury and property damage, including products and completed operations coverage with an aggregate limit of at least two million dollars (\$2,000,000).

b. Workers' Compensation and Employer Liability Insurance

- 1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:
  - i. Workers' compensation in an amount not less than one million dollars (\$1,000,000) including employer liability of one million dollars (\$1,000,000) per accident for bodily injury by accident, one million dollars (\$1,000,000) policy limit by disease, and one million dollars (\$1,000,000) per employee for bodily injury by disease.
- 2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:
  - i. The Contractor employs fewer than five (5) employees;
  - ii. The Contractor is a sole proprietor;
  - iii. The Contractor is in the construction business or trades with no employees;
  - iv. The Contractor is in the coal mining industry with no employees;
  - v. The Contractor is a state or local government; or
  - vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Automobile Liability Insurance

- 1) The Contractor shall maintain automobile liability insurance which shall cover liability arising out of any automobile (including owned, leased, hired, and non-owned automobiles).

- 2) The Contractor shall maintain bodily injury/property damage with a limit not less than one million dollars (\$1,000,000) per occurrence or combined single limit.

D.33. Major Procurement Contract Sales and Use Tax. Pursuant to Tenn. Code Ann. § 4-39-102 and to the extent applicable, the Contractor and the Contractor's subcontractors shall remit sales and use taxes on the sales of goods or services that are made by the Contractor or the Contractor's subcontractors and that are subject to tax.

**E. SPECIAL TERMS AND CONDITIONS:**

E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.

E.2. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.

The obligations set forth in this Section shall survive the termination of this Contract.

E.3. Intellectual Property Indemnity. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

E.4. Software License Warranty. Contractor grants a license to the State to use all software provided under this Contract in the course of the State's business and purposes.

E.5. Software Support and Maintenance Warranty. Contractor shall provide to the State all software upgrades, modifications, bug fixes, or other improvements in its software that it makes generally available to its customers.

E.6. Family Educational Rights and Privacy Act & Tennessee Data Accessibility, Transparency and Accountability Act. The Contractor shall comply with the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. 1232(g)) and its accompanying regulations (34 C.F.R. § 99) ("FERPA"). The Contractor warrants that the Contractor is familiar with FERPA requirements and that it will comply with these requirements in the performance of its duties under this Contract. The Contractor agrees to cooperate with the State, as required by FERPA, in the performance of its duties under this Contract. The Contractor agrees to maintain the confidentiality of all education

records and student information. The Contractor shall only use such records and information for the exclusive purpose of performing its duties under this Contract.

The Contractor shall also comply with Tenn. Code Ann. § 49-1-701, *et seq.*, known as the "Data Accessibility, Transparency and Accountability Act," and any accompanying administrative rules or regulations (collectively "DATAA"). The Contractor agrees to maintain the confidentiality of all records containing student and de-identified data, as this term is defined in DATAA, in any databases, to which the State has granted the Contractor access, and to only use such data for the exclusive purpose of performing its duties under this Contract.

Any instances of unauthorized disclosure of data containing personally identifiable information in violation of FERPA or DATAA that come to the attention of the Contractor shall be reported to the State within twenty-four (24) hours. Contractor shall indemnify and hold harmless State, its employees, agents and representatives, from and against any and all claims, liabilities, losses, or causes of action that may arise, accrue, or result to any person or entity that is injured or damaged as a result of Contractor's failure to comply with this section.

- E.7. Prohibited Advertising or Marketing. The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.
- E.8. Personally Identifiable Information. While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify and/or procure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for

individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law.

**IN WITNESS WHEREOF,**

**TEACHSTONE TRAINING, LLC:**

Scott Guengerich 1-8-17  
CONTRACTOR SIGNATURE DATE

Scott Guengerich Sr Director of Finance  
PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

**TENNESSEE DEPARTMENT OF EDUCATION:**

Candice McQueen JC 1/9/18  
CANDICE MCQUEEN, COMMISSIONER DATE

## ATTACHMENT A

## ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

<p>If the attestation applies to more than one contract, modify this row accordingly.</p> <p>SUBJECT CONTRACT NUMBER:</p>	
<p>CONTRACTOR LEGAL ENTITY NAME:</p>	Teachstone Training
<p>EDISON VENDOR IDENTIFICATION NUMBER:</p>	

If the attestation applies to more than one contract, modify the following paragraph accordingly.

**The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.**



CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

Scott Guengerich Sr. Director of Finance

PRINTED NAME AND TITLE OF SIGNATORY

1-8-2017

DATE OF ATTESTATION

Attachment B

Enterprise Information Security Policies



**State of  
Tennessee Department of Finance and  
Administration Strategic Technology  
Solutions Information Security Program**

*Document Version 2.1 – December 15, 2016*

## Table of Contents

	<u>Page</u>
<b>1. EXECUTIVE SUMMARY</b>	<b>1</b>
<b>2. INTRODUCTION</b>	<b>2</b>
Scope (2.1)	3
Authority (2.2)	3
Exceptions (2.3)	4
Review (2.4)	4
Document Format (2.5)	4
Policy Maintenance (2.6)	4
<b>3. INFORMATION SECURITY POLICIES</b>	<b>5</b>
Management Direction for Information Security (3.1)	5
Policies for Information Security (3.1.1)	5
Policies for Information Security (3.1.2)	5
Policies for Information Security (3.1.3)	5
<b>4. OPERATIONS SECURITY</b>	<b>5</b>
Operational Procedures and Responsibilities (4.1)	5
Documented Operating Procedures (4.1.1)	5
Change Management (4.1.2)	6
Change Control Procedures (4.1.2.1)	6
Capacity Management (4.1.3)	6
Separation of Development, Testing and Operational Environments (4.1.4)	6
Protection from Malware (4.2)	6
Malicious Software Control (4.2.1)	6
Backup (4.3)	6
Data Backup (4.3.1)	6
Logging and Monitoring (4.4)	7
Event Logging (4.4.1)	7
Availability and Performance Monitoring (4.4.2)	7
Protection of Log Information (4.4.3)	7
Administrator and Logs (4.4.4)	7
Clock Synchronization (4.4.5)	7
Control of Operational Software (4.5)	7
Installation of Software on Operational Systems (4.5.1)	7
Patch Management (4.5.1.1)	7
Software Development Code (4.5.1.2)	8
Review of Application and Operating System Changes (4.5.1.3)	8
Technical and Vulnerability Management (4.6)	8
Management of Technical Vulnerabilities (4.6.1)	8
Restrictions on Software Installation (4.6.2)	8
Information Systems Audit Considerations (4.7)	8

Information Systems Audit Controls (4.7.1)	8
<b>5. ACCESS CONTROL</b>	<b>9</b>
Business Requirements of Access Control (5.1)	9
Access Control Policy (5.1.1)	9
Access to Networks and Network Services (5.1.2)	9
Remote Access (5.1.2.1)	9
Information Security Roles and Responsibilities (5.1.3)	9
Segregation of Duties (5.1.4)	9
User Access Management (5.2)	9
User Registration and De-Registration (5.2.1)	9
User Access Provisioning (5.2.2)	9
User Account Naming (5.2.2.1)	10
Management of Privileged Access Rights (5.2.3)	10
Management of Secret Authentication of Information Users (5.2.4)	10
Review of User Access Rights (5.2.5)	10
Removal or Adjustment of Access Rights (5.2.6)	10
User Responsibilities (5.3)	10
Use of Secret Authentication Information (5.3.1)	10
System and Application Access Control (5.4)	10
Information Access Restriction (5.4.1)	10
Secure Log-on Procedures (5.4.2)	11
System Administrator Access (5.4.2.1)	11
Logon Banner (5.4.2.2)	11
Service Account Use (5.4.2.3)	11
Password Management System (5.4.3)	11
Use of Privileged Utility Programs (5.4.4)	11
Access Control to Program Source Code (5.4.5)	11
Default Configurations (5.4.6)	11
<b>6. ASSET MANAGEMENT</b>	<b>12</b>
Responsibility for Assets (6.1)	12
Inventory of Assets (6.1.1)	12
Ownership of Assets (6.1.2)	12
Acceptable Use of Assets (6.1.3)	12
Return of Assets (6.1.4)	12
Asset Identification (6.1.5)	12
Data Classification (6.2)	12
Classification of Data (6.2.1)	12
Labelling of Data (6.2.2)	12
Handling and Use of Data (6.2.3)	12
Public Data Classification and Control (6.2.3.1)	13
Confidential Data Classification and Control (6.2.3.3)	13
Confidential Data on Personally Owned Devices (6.2.3.4)	13
Confidential Electronic Messages Classification and Control (6.2.3.5)	13
Payment Card Information Classification and Control (6.2.3.6)	13
Use of Confidential Data (6.2.3.7)	14
Media Handling (6.3)	14

Management of Removable Media (6.3.1)	14
Repair of Removable Media (6.3.1.1)	14
Disposal of Removable Media (6.3.2)	14
Physical Transfer of Removable Media (6.3.3)	14
Workstation Computing (6.4)	14
State Provided Workstation Computing Platforms (6.4.1)	14
Workstation Platform Reassignment (6.4.2)	15
Workstation Platform Disposal (6.4.3)	15
Cloud Services (6.4.4)	15
<b>7. PHYSICAL AND ENVIRONMENTAL SECURITY</b>	<b>15</b>
Secure Areas (7.1)	15
Physical Security Perimeter (7.1.1)	15
Physical Entry Controls (7.1.2)	15
Securing Offices, Rooms and Facilities (7.1.3)	16
Protecting against External and Environmental Threats (7.1.4)	16
Working in Secure Areas (7.1.5)	16
Delivery and Loading Areas (7.1.6)	16
Equipment (7.2)	16
Equipment Siting and Protection (7.2.1)	16
Supporting Utilities (7.2.2)	16
Cabling Security (7.2.3)	16
Equipment Maintenance (7.2.4)	16
Removal of Assets (7.2.5)	16
Security of Equipment and Assets Off-Premises (7.2.6)	17
Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)	17
Unattended User Equipment (7.2.8)	17
Session Time Outs (7.2.8.1)	17
Clear Desk and Clear Screen Policy (7.2.9)	17
<b>8. NETWORK CONNECTIVITY SECURITY</b>	<b>18</b>
Network Security Management (8.1)	18
Network Controls (8.1.1)	18
Security of Network Services (8.1.2)	18
Segregation in Networks (8.1.3)	18
Information Transfer (8.2)	18
Information Transfer Policies and Procedures (8.2.1)	18
Agreements on Data Transfer Policies (8.2.2)	18
Electronic Messaging (8.2.3)	19
Internal Electronic Messages Control (8.2.3.1)	19
External Electronic Messages Control (8.2.3.2)	19
Electronic Messaging Management (8.2.3.3)	19
Confidentiality or Non-Disclosure Agreements (8.2.4)	19
<b>9. MOBILE DEVICE SECURITY POLICY</b>	<b>20</b>
Mobile Devices and Teleworking (9.1)	20
Mobile Device Policy (9.1.1)	20

	Teleworking (9.1.2)	20
10.	<b>EXTERNAL PARTY SECURITY</b>	<b>21</b>
	Information Security for External Party Relationships (10.1)	21
	Information Security Policy for External Party Relationships (10.1.1)	21
	Identification of Risk (10.1.2)	21
	Addressing Security within External Party Agreements (10.1.3)	21
	Reporting of Security Incidents (10.1.3.1)	21
	Sub-Contractors Requirements (10.1.3.2)	21
	Addressing Security for Access to Citizen Data (10.1.4)	21
11.	<b>SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE</b>	<b>22</b>
	Security Requirements of Information Systems (11.1)	22
	Security Requirements of Information Systems (11.1.1)	22
	Securing Application Services on Public Networks (11.1.2)	22
	Protecting Application Services Transactions (11.1.3)	22
	Information Security in Project Management (11.1.4)	22
	Security in Development and Support Processes (11.2)	22
	Security Requirements of Information Systems (11.2.1)	22
	Security in Application Systems Development (11.2.1.1)	23
	Input and Data Validation (11.2.1.2)	23
	Output Data Validation (11.2.1.3)	23
	Application Authorization (11.2.1.4)	23
	Inter-process Message Authentication (11.2.1.5)	23
	Control of Internal Processing (11.2.1.6)	23
	System Change Control Procedures (11.2.2)	23
	Technical Review of Applications after Operating Platform Changes (11.2.3)	23
	Restrictions or Changes to Software Packages (11.2.4)	24
	Secure System Engineering Principles (11.2.5)	24
	Secure Development Environment (11.2.6)	24
	Outsourced Development (11.2.7)	24
	System Security Testing (11.2.8)	24
	System Acceptance Testing (11.2.9)	24
	Test Data (11.3)	24
	Protection of Test Data (11.3.1)	24
12.	<b>BUSINESS CONTINUITY MANAGEMENT</b>	<b>25</b>
	Information Business Continuity (12.1)	25
	Planning Information Systems Continuity (12.1.1)	25
	Business Impact Analysis (12.1.1.1)	25
	Critical Applications (12.1.1.2)	25
	Non-Critical Applications (12.1.1.3)	25
	Implementing Information Systems Continuity (12.1.2)	25
	Verify, Review and Evaluate information Systems Continuity (12.1.3)	25
	Redundancies (12.2)	25
	Availability of Information Processing Facilities (12.2.1)	25

<b>13.</b>	<b>INFORMATION SECURITY INCIDENT MANAGEMENT</b>	<b>26</b>
	<b>Management of Information Security Incidents and Improvements (13.1)</b>	<b>26</b>
	<b>Responsibilities and Procedures (13.1.1)</b>	<b>26</b>
	<b>Reporting Information Security Events (13.1.2)</b>	<b>27</b>
	<b>Data Breach and Disclosure (13.1.2.1)</b>	<b>27</b>
	<b>Reporting Information Security Weakness (13.1.3)</b>	<b>27</b>
	<b>Assessment of and Decision on Information Security Events (13.1.4)</b>	<b>27</b>
	<b>Response to Information Security Incidents (13.1.5)</b>	<b>27</b>
	<b>Learning from Information Security Incidents (13.1.6)</b>	<b>27</b>
	<b>Collection of Evidence (13.1.7)</b>	<b>27</b>
<b>14.</b>	<b>CRYPTOGRAPHY</b>	<b>28</b>
	<b>Cryptographic Controls (14.1)</b>	<b>28</b>
	<b>Use of Cryptographic Controls (14.1.1)</b>	<b>28</b>
	<b>Transmission Integrity (14.1.2)</b>	<b>28</b>
	<b>Transmission Confidentiality (14.1.3)</b>	<b>28</b>
	<b>Cryptographic Module Authentication (14.1.4)</b>	<b>28</b>
	<b>Cryptographic Module Authentication (14.1.5)</b>	<b>28</b>
	<b>Key Management (14.1.6)</b>	<b>29</b>
<b>15.</b>	<b>COMPLIANCE</b>	<b>30</b>
	<b>Compliance with Legal and Contractual Requirements (15.1)</b>	<b>30</b>
	<b>Identification of Applicable Legislation and Contractual Requirements (15.1.1)</b>	<b>30</b>
	<b>Intellectual Property Rights (15.1.2)</b>	<b>30</b>
	<b>Protection of Records (15.1.3)</b>	<b>30</b>
	<b>Privacy and Protection of Personally Identifiable Information (15.1.4)</b>	<b>30</b>
	<b>Regulation of Cryptographic Controls (15.1.5)</b>	<b>30</b>
	<b>Information Security Reviews (15.2)</b>	<b>30</b>
	<b>Independent Review of Information Security (15.2.1)</b>	<b>30</b>
	<b>Compliance with Security Policies and Standards (15.2.2)</b>	<b>31</b>
	<b>Technical Compliance Review (15.2.3)</b>	<b>31</b>
<b>16.</b>	<b>HUMAN RESOURCE</b>	<b>32</b>
	<b>Prior to Employment (16.1)</b>	<b>32</b>
	<b>Screening (16.1.1)</b>	<b>32</b>
	<b>Acceptable Use Policy (16.1.2)</b>	<b>32</b>
	<b>During Employment (16.2)</b>	<b>32</b>
	<b>Management Responsibilities (16.2.1)</b>	<b>32</b>
	<b>Information Security Awareness, Education and Training (16.2.2)</b>	<b>32</b>
<b>17.</b>	<b>VERSION HISTORY</b>	<b>33</b>
<b>18.</b>	<b>TERMS AND DEFINITIONS</b>	<b>34</b>
<b>19.</b>	<b>APPENDICES</b>	<b>36</b>

## 1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the confidentiality, integrity and availability of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been created to establish and uphold the minimum requirements that are necessary to protect information resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased or controlled by, or operated on behalf of the State of Tennessee. The methodologies and practices of external entities that require access to the State Tennessee's information resources may be impacted and could be included in this scope. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) controlled by or operated on behalf of the State of Tennessee where lawfully permitted.
- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) owned by the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

This document applies to all full- and part-time employees of the State of Tennessee, all third parties, contractors or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency information technology (IT) professionals and approval by the Chief Information Security Officer (CISO) and executive management team within Strategic Technology Solutions, Department of Finance and Administration

All information resources and any information system owned by the State of Tennessee should be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the State government and those they serve. Access to information technology assets will be granted using the principle of least privilege.

All of the approved policies will support the requirements of the Information Systems Council of the State of Tennessee.

## 2. INTRODUCTION

### The Information Security Challenge

Information technology (IT) solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and technologies that support business processes at a low cost is a foundational component of successful IT programs. This integration moves quickly to align itself with the "just in time" requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes bypassing existing processes to meet time demands of the customers whom they serve. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need to evaluate risk and has established information security programs. One of the main goals of any successful information security program is to protect the organization's revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy to list a few.

Security policies are a foundational component of any successful security program. The Enterprise Information Security Policies for the State of Tennessee are based on the International Standards Organization (ISO) 27002 standard framework. The policies are designed to comply with applicable statutes and regulations; however, if there is a conflict, applicable statutes and regulations will take precedence. The policies included in this document are to be considered the minimum requirements for providing a secure operational environment.

## **Scope (2.1)**

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- All computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

All full- and part-time employees of the State of Tennessee, all third parties, contractors, or vendors who work on state premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data should adhere to the policies and requirements set forth in this document.

## **Authority (2.2)**

The Information Systems Council (ISC) has authorized the Department of Finance and Administration, Strategic Technology Solutions (STS) to establish and enforce enterprise policies and standards as they are related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network. Strategic Technology Solutions is responsible and authorized by the ISC to perform audits on any device that attaches to the State of Tennessee's enterprise network.

### Reference:

*Tennessee Code Annotated, Section 4-3-5501, effective, May 10, 1994 ISC  
Information Resource Policies, Policy 1.00  
ISC Information Resource Policies, Policy 13.00*

### **Exceptions (2.3)**

All exceptions to any of the security policies will be reviewed, evaluated and processed by a member of the Chief Information Security Officer's staff.

### **Review (2.4)**

Review of this document takes place within Security Advisory Council sessions and will occur on an annual basis at a minimum. Document review can also be requested by sending a request to the Chief Information Security Officer.

The official policy document and supporting documentation will be published on the STS intranet site located at:

<https://www.teamtn.gov/content/dam/teamtn/sts/sts-documents/Enterprise-Information-Security-Policies-ISO-27002-Internal.pdf>

### **Document Format (2.5)**

This document generally follows the International Standards Organization (ISO) 27002 (2013) standard framework for information technology security management. Each section starts with a high-level security control category followed by the control objective. Policy statements follow the objectives.

The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise.

## **X. Section Name**

**Control Category (x.x)**  
Objective Statement

**Policy Name (x.x.x)**  
Policy Statement

**Sub-Policy Name (x.x.x.x)**  
Sub-Policy Statement

### **MINIMUM COMPLIANCE REQUIREMENTS:Policy Maintenance (2.6)**

All policies will be maintained in accordance with the STS policy process documentation.

### 3. INFORMATION SECURITY POLICIES

#### **Management Direction for Information Security (3.1)**

Objective: To provide management direction and support for information security in accordance with agency business requirements and relevant state and federal statute and regulations for the State of Tennessee's computing environments.

#### **Policies for Information Security (3.1.1)**

STS Information Security Management will initiate and control an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework and a security technology framework.

#### **Policies for Information Security (3.1.2)**

Agencies should develop agency specific policy documents as required by agency or regulatory requirement provided the minimum requirements set forth in this document are met.

#### **Policies for Information Security (3.1.3)**

Agencies are responsible for communicating this policy document throughout their respective agencies.

### 4. OPERATIONS SECURITY

#### **Operational Procedures and Responsibilities (4.1)**

Objective: To protect critical State information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction to ensure correct and proper operations.

#### **Documented Operating Procedures (4.1.1)**

All agencies of the State of Tennessee and vendors or contractors acting on behalf of the State should identify, document and maintain standard security operating procedures and configurations for their respective operating environments and ensure the documentation is available to all users who need it.

## **Change Management (4.1.2)**

Changes to information processing facilities and systems should be controlled and monitored for security compliance. Formal management responsibilities and procedures should exist to ensure satisfactory control of all changes to equipment, software, configurations or procedures that affect the security of the State of Tennessee's operational environment. All written documentation generated by the change control policies and procedures should be retained as evidence of compliance.

### **Change Control Procedures (4.1.2.1)**

Change control procedures should include authorization, risk assessment, logging, audit ability, and roll back procedures.

## **Capacity Management (4.1.3)**

The use of resources should be monitored and tuned so that projections of future capacity requirements can be made.

## **Separation of Development, Testing and Operational Environments (4.1.4)**

Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and should not be used in development or test environments.

## **Protection from Malware (4.2)**

Objective: Prevent the automated propagation of malicious code and contamination of environments attached to the enterprise network.

### **Malicious Software Control (4.2.1)**

All computing platforms that are attached to the State's enterprise technology infrastructure or operated on behalf of the State should be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses, logic bombs and rootkits. Compromised systems should be removed from the operational environment.

## **Backup (4.3)**

Objective: To prevent loss of data and to ensure data availability.

### **Data Backup (4.3.1)**

Backup copies of data, software and system images should be taken and tested regularly in accordance with established procedures. A copy of the backup data should be stored off-site according to applicable regulatory requirements and State policy. Results of restore tests should be furnished to data owners with recommendations for any remedial steps found. Data owners should approve any remedial plans and timelines for implementing those remediation steps within a reasonable period not to exceed three months. Following remediation, the restore testing should be repeated and results documented to ensure that those steps mitigated all identified issues.

## **Logging and Monitoring 4.4)**

Objective: To record events and generate evidence.

### **Event Logging (4.4.1)**

All systems should be configured to support security event logging, recording user activities, exceptions, faults and information security events. System administrators should monitor and take appropriate action for inappropriate access. Mission critical systems should be configured to support automated logging to a facility that protects the integrity of the logs. Logging levels and monitored elements will be configured in accordance with federal and state statute and regulatory requirements.

### **Availability and Performance Monitoring (4.4.2)**

Mission critical systems should be configured to support Teachstone approved automated monitoring of system availability and performance.

### **Protection of Log Information (4.4.3)**

Logging facilities and log information should be protected against tampering and unauthorized access.

### **Administrator and Logs (4.4.4)**

System administrator activities should be logged and the logs protected and regularly reviewed.

## **Control of Operational Software (4.5)**

Objective: To ensure the integrity of operational systems.

### **Patch Management (4.5.1.1)**

All applications and processing devices that are attached to the State's enterprise technology infrastructure will have critical application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable

ate can be agreed upon by all affected parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

### **Review of Application and Operating System Changes (4.5.1.3)**

Applications and operating systems should be reviewed and tested to ensure that there is no adverse impact on operations or security when a change has been performed on the operating system. (e.g. patch).

## **Technical and Vulnerability Management (4.6)**

Objective: To prevent the exploitation of technical vulnerabilities.

### **Management of Technical Vulnerabilities (4.6.1)**

Information about technical vulnerabilities on information systems and supporting infrastructure should be obtained in a timely fashion, evaluated for exposure and risk and appropriate measures implemented to address the associated risk.

## **Information Systems Audit Considerations (4.7)**

Objective: To minimize the impact of audit activities on operational systems.

### **Information Systems Audit Controls (4.7.1)**

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed upon in advance to minimize disruptions to business processes.

## 5. ACCESS CONTROL

### **Business Requirements of Access Control (5.1)**

Objective: To limit access to information and information processing facilities.

#### **Access Control Policy (5.1.1)**

All access rules and requirements to access Teachstone's information resources should be developed, documented and maintained by their respective resource owners. Access to the State of Tennessee's information resources will be granted consistent with the concept of least privilege. All information processing systems owned by or operated on behalf of Teachstone should have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to data resources that they are explicitly authorized to use.

#### **Access to Networks and Network Services (5.1.2)**

All access and connectivity to Teachstone's enterprise network or networks operated on behalf of Teachstone should be granted consistent with the concept of least privilege. Users will only be provided with access to the network and network resources that they have been specifically authorized to use.

#### **Information Security Roles and Responsibilities (5.1.3)**

All information security responsibilities should be defined and assigned by the access granting authority.

#### **Segregation of Duties (5.1.4)**

Where appropriate, conflicting duties and areas of responsibility should be segregated and assigned to different individuals to reduce opportunities for unauthorized or unintentional modification or misuse of the State's assets.

### **User Access Management (5.2)**

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

#### **User Registration and De-Registration (5.2.1)**

A formal user registration and de-registration process should be implemented to enable assignment of access rights and to adjust those rights as the user's role changes.

#### **User Access Provisioning (5.2.2)**

User access to information resources should be authorized and provisioned according to Teachstone's employee provisioning process.

### **Management of Privileged Access Rights (5.2.3)**

Users should have the least privileges required to perform their roles as identified and approved by their agency. The allocation and use of privileged access rights should be restricted and controlled.

### **Management of Secret Authentication of Information Users (5.2.4)**

The allocation of secret authentication information should be controlled through a formal management process.

### **Review of User Access Rights (5.2.5)**

A user's access rights should be reviewed, validated and updated for appropriate access by their section supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies). removal or

### **Adjustment of Access Rights (5.2.6)**

All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment; contract, agreement or change of agency by the close of business on the user's last working day.

## **User Responsibilities (5.3)**

Objective: To make users accountable for safeguarding their authentication information.

### **Use of Secret Authentication Information (5.3.1)**

Users should follow State policy in the use of secret authentication information.

## **System and Application Access Control (5.4)**

Objective: To prevent unauthorized access to systems and applications.

### **Information Access Restriction (5.4.1)**

Access to information and application system function should be restricted in accordance with the defined access control policy.

### **Secure Log-on Procedures (5.4.2)**

Where required by the access control policy, access to systems and application should be controlled by a secure log-on procedure. At a minimum, user access to protected information resources requires the utilization of User Identification (UserID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

### **System Administrator Access (5.4.2.1)**

–Teachstone will use a multi-factor solution to obtain administrator access.

Service accounts should be unique to each application and/or system and should only be used to authenticate systems and/or applications to specific services.

### **Password Management System (5.4.3)**

Password management systems should be interactive and should ensure quality passwords. Use of Privileged Utility Programs (5.4.4)

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

### **Access Control to Program Source Code (5.4.5)**

Access to program source code should be restricted to authorized users.

### **Default Configurations (5.4.6)**

All applications and processing devices that are attached to Teachstone's enterprise technology infrastructure should be deployed with modified configurations for, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification or destruction.

## **MINIMUM REQUIREMENTS:**

Redacted for public version of policy

## 6. ASSET MANAGEMENT Responsibility for Assets

### (6.1)

Objective: To identify organizational assets and define appropriate protection responsibilities.

**RESERVED (6.1.1)**

**RESERVED (6.1.2)**

### **Acceptable Use of Assets (6.1.3)**

Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented, implemented and communicated to the employees and contractors who have access to those assets.

### **Data Classification (6.2)**

Objective: To ensure the data used and managed by the State receives an appropriate level of protection commensurate with the value, importance and criticality of the data to the State

#### **Classification of Data (6.2.1)**

Data assets owned and/or managed by the State of Tennessee should be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable state and/or federal statute or regulations to indicate the need, priorities and degree of protection it will receive. At a minimum, data will be classified as Public or Confidential.

#### **Labelling of Data (6.2.2)**

An appropriate set of procedures for labeling data assets owned and/or managed by the State of Tennessee should be developed and implemented in accordance with the State's data classification scheme.

#### **Handling and Use of Data (6.2.3)**

Procedures for handling data assets should be developed and implemented in accordance with the data classification scheme adopted by the State.

### **Public Data Classification and Control (6.2.3.1)**

Data classified as public should be protected from unauthorized modification or destruction.

### **Confidential Data Classification and Control (6.2.3.3)**

Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and cannot be used in development or test environments or publicly disclosed. Controls should be applied to data in a manner consistent with its value, sensitivity and criticality to the business and operation of state government. Data classified as confidential must be encrypted at rest and during transmission in accordance with applicable state or federal statute or regulatory requirements.

### **Confidential Data on Personally Owned Devices (6.2.3.4)**

Confidential data should not be stored on personally owned computing platforms or on personally owned mobile computing platforms unless managed by Teachstone's mobile device management solution.

### **Confidential Electronic Messages Classification and Control (6.2.3.5)**

E-mail sent from Teachstone's domain out through the public Internet must be encrypted if it contains confidential information in the body or attachment. Confidential information should not be placed into the subject line of the message.

### **Payment Card Information Classification and Control (6.2.3.6)**

Payment card information must be considered confidential when an individual's first name or first initial and last name are present in combination with account number, credit or debit card number, required security code, access code, or password that would permit access to an individual's financial account. (Payment Card Industry Data Security Standard [https://www.pcisecuritystandards.org/security\\_standards/](https://www.pcisecuritystandards.org/security_standards/))

The Payment Card Industry – Data Security Standards (PCI DSS) comprise a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector statutes and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional statutes, government regulations, or other legal requirements.

All payment card information stored and processed by the State, or transmitted over State networks must be in compliance with the PCI-DSS. Storage of the full Primary Account Number (PAN) on State systems is prohibited. Agencies that use payment card services should also comply with statewide accounting policies as documented by the Department of Finance and Administration, Division of Accounts.

### **Use of Confidential Data (6.2.3.7)**

The use of confidential data will only be permitted in production systems. The use of confidential data is prohibited from training, test, and development systems.

To reduce the risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test, and operational facilities. Confidential data should not be copied into test and development systems. Development and test environments should not be directly connected to production environments. Data and operational software test systems should emulate production systems as closely as possible.

**Media Handling (6.3) Objective:** To prevent unauthorized disclosure, modification, removal or destruction of data stored on media.

### **Management of Removable Media (6.3.1)**

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

#### **Repair of Removable Media (6.3.1.1)**

Removable media containing state data should be sanitized prior to removing it from Teachstone facilities for maintenance or repair

#### **Disposal of Removable Media (6.3.2)**

Removable media should be disposed of securely when no longer required, using approved State procedures.

#### **Physical Transfer of Removable Media (6.3.3)**

Removable media containing sensitive or confidential data must be protected against unauthorized access, misuse or corruption during transport.

**Workstation Computing (6.4)** Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on user assigned processing devices.

#### **State Provided Workstation Computing Platforms (6.4.1)**

Workstation computing platforms, including laptops should be physically protected against theft when left unattended. Workstation computing platforms should not store confidential data assets where it is not absolutely necessary to perform the specific job related duties. Storage of confidential data assets on a workstation computing platform should have approval from the asset custodian for such storage. Confidential data assets which have been authorized to be stored on the local workstation should be encrypted while stored on the workstation computing platform.

#### **Workstation Platform Reassignment (6.4.2)**

All workstation computing platforms including all external storage devices should be sanitized prior to being re-issued or re-purposed to another employee.

#### **Workstation Platform Disposal (6.4.3)**

Hard drives in workstation computing platforms including all mobile storage devices should be sanitized using approved sanitization procedures or destroyed prior to transfer or surplus of processing device to non-State agencies.

## **7. PHYSICAL AND ENVIRONMENTAL SECURITY**

### **Secure Areas (7.1)**

Objective: To prevent unauthorized physical access, damage and interference to the State's information and information processing facilities.

#### **Physical Security Perimeter (7.1.1)**

All enterprise data processing facilities that process or store data classified as critical or sensitive should have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All other processing facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

#### **Physical Entry Controls (7.1.2)**

Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.

### **Securing Offices, Rooms and Facilities (7.1.3)**

Physical security for offices, rooms and facilities should be designed and applied commensurate with the classification and value of the data being handled or processed.

### **Protecting against External and Environmental Threats (7.1.4)**

Physical protection against natural disaster, malicious attack or accidents should be considered and incorporated in facility design, construction and placement.

### **Working in Secure Areas (7.1.5)**

Procedures for working in secure areas should be created and implemented.

### **Delivery and Loading Areas (7.1.6)**

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.

## **Equipment (7.2)**

Objective: To prevent loss, damage, theft or compromise of assets or an interruption to State operations.

### **Equipment Siting and Protection (7.2.1)**

Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Equipment located in areas where Teachstone is unable to maintain a secure perimeter should be locked in a secured manner with access controlled by Teachstone. Secured cabinets or facilities should support further segregation within Teachstone's Information Technology (IT) organization based on role and responsibility.

### **Supporting Utilities (7.2.2)**

Infrastructure and related computing equipment should be protected from power failures and other disruptions by failures in supporting utilities.

### **Cabling Security (7.2.3)**

Power and telecommunications cable carrying data or supporting information services should be protected from interception, interference or damage.

### **Equipment Maintenance (7.2.4)**

Equipment should be correctly maintained to ensure its continued availability and integrity.

### **Removal of Assets (7.2.5)**

All equipment, software or information that is a part of State operational systems or processes should not be taken off-site without the prior authorization from executive management or a

designated representative and should be removed according to documented agency equipment transfer procedures.

### **Security of Equipment and Assets Off-Premises (7.2.6)**

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

### **Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)**

All data processing equipment including storage devices subject to transfer or reuse should be sanitized in accordance with the State of Tennessee's media reuse procedure or superseding state or federal requirements. Data processing equipment assets that are not subject to transfer or reuse should be destroyed in accordance with the State of Tennessee's media disposal procedures or in accordance with superseding state or federal requirements.

### **Unattended User Equipment (7.2.8)**

Users should ensure that unattended data processing equipment has appropriate protection.

#### **Session Time Outs (7.2.8.1)**

All systems and devices owned and operated by or on behalf of Teachstone should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

### **Clear Desk and Clear Screen Policy (7.2.9)**

All data classified as confidential must be stored in a locked cabinet or room when unattended. All data processing equipment that provide access to Information Processing Systems will be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended.

All computing platforms residing in non-secured facilities with attached displays should be oriented away from direct line of sight from unauthorized viewers.

### **MINIMUM COMPLIANCE REQUIREMENTS:**

**Redacted for public version of policy**

## 8. NETWORK CONNECTIVITY SECURITY

### **Network Security Management (8.1)**

Objective: To ensure the protection of the State's assets that are accessible by suppliers and vendors.

#### **Network Controls (8.1.1)**

Networks should be managed and controlled to protect information in systems and applications.

#### **Security of Network Services (8.1.2)**

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

#### **Segregation in Networks (8.1.3)**

All enterprise network architectures operated by, or on behalf of, Teachstone should be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones should be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by Director of Software Engineering.

### **Information Transfer (8.2)**

Objective: To maintain the security of information transferred within network infrastructures manage by on behalf of the State and with any external entity.

#### **Information Transfer Policies and Procedures (8.2.1)**

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

#### **Agreements on Data Transfer Policies (8.2.2)**

Agreements should address the secure transfer of business information between the State and external parties.

### **Electronic Messaging (8.2.3)**

Data involved in electronic messaging should be appropriately protected.

#### **Internal Electronic Messages Control (8.2.3.1)**

Email and instant messages internal to the State's domain containing confidential data should be encrypted during transmission. Confidential information should not be placed into the subject line of email or as any part of instant messages.

#### **External Electronic Messages Control (8.2.3.2)**

E-mail sent through the public Internet must be encrypted if it contains confidential information in the body or attachment of the email. Confidential information should not be placed into the subject line of the message.

#### **Electronic Messaging Management (8.2.3.3)**

All electronic messages created, sent or received in conjunction with the transaction of official business should use Teachstone approved gateway(s) to communicate via the Internet.

### **Confidentiality or Non-Disclosure Agreements (8.2.4)**

When exchanging or sharing information classified as Sensitive or Confidential with external parties that are not already bound by the contract confidentiality clause, a non-disclosure agreement should be established between the owner of the data and the external party.

Note: Agencies should work with agency legal counsel to ensure proper language is used.

## 9. MOBILE DEVICE SECURITY POLICY

**Mobile Devices and Teleworking (9.1) Objective:** To ensure the security of teleworking and the use of mobile devices.

### **Mobile Device Policy (9.1.1)**

All mobile devices that connect to Teachstone's managed data or infrastructure should be managed by the State's enterprise mobile device management solution or the State's enterprise configuration manager and should comply with appropriate mobile device usage policies as required by state or federal statute or regulation.

### **Teleworking (9.1.2)**

Teleworkers should comply with the appropriate telework policies as required by state or federal statute, regulation, state or agency policy.

## **10. EXTERNAL PARTY SECURITY**

### **Information Security for External Party Relationships (10.1)**

Objective: To ensure the protection of Teachstone's assets that are accessed, processed, communicated to, or managed by external parties, suppliers or vendors. This includes any external party who has access to physical data processing facilities, logical access to Teachstone's data processing systems via local or remote access or access via another external party into Teachstone's data processing facilities.

#### **Information Security Policy for External Party Relationships (10.1.1)**

Information and physical security requirements for mitigating the risks associated with supplier or vendor access to Teachstone's assets should be agreed upon in writing with the external party. All external parties must agree in writing to comply with all applicable information security policies, confidentiality agreements, third party connectivity agreements, executive orders, standards, controls and regulations.

#### **Identification of Risk (10.1.2)**

Risk involving external parties should be identified and proper controls implemented prior to the granting of access to any Teachstone information, information technology asset or information process facility.

#### **Addressing Security within External Party Agreements (10.1.3)**

All relevant information security requirements should be established and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT infrastructure components for Teachstone's processing systems or infrastructure

##### **Reporting of Security Incidents (10.1.3.1)**

External Party Agreements will require external parties to report perceived security incidents that may impact the confidentiality, integrity or availability of State data immediately.

##### **Sub-Contractors Requirements (10.1.3.2)**

Primary external parties should require their sub-contractors to abide by State of Tennessee policies and security requirements, as applicable.

#### **Addressing Security for Access to Citizen Data (10.1.4)**

Risk involving external party access to citizen data should be identified and proper controls implemented prior to the granting of access to any State of Tennessee citizen data. Appropriate controls should be agreed upon, documented in external party agreements and implemented prior to the granting of access to any citizen data.

## 11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

### **Security Requirements of Information Systems (11.1)**

Objective: To ensure that information security is an integral part of information systems throughout their life cycle. This includes application infrastructure, vendor applications, agency-developed, and user-developed applications and information systems which provide services over public networks or the State's internal network.

#### **Security Requirements of Information Systems (11.1.1)**

Security requirements should be identified and documented as part of the overall business case for new information systems and for enhancement to existing information systems and should be included early and continuously throughout the lifecycle of the application, including, but not limited to the conception, design, development, testing, implementation, maintenance and disposal phases.

#### **Securing Application Services on Public Networks (11.1.2)**

Information involved in application services passing over public networks should be protected from fraudulent activity and unauthorized disclosure or modification.

#### **Protecting Application Services Transactions (11.1.3)**

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

#### **Information Security in Project Management (11.1.4)**

Information security should be addressed at project initiation and throughout the lifecycle of the project.

### **Security in Development and Support Processes (11.2)**

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

#### **Security Requirements of Information Systems (11.2.1)**

Requirements, rules and guidelines for the development of software and systems should be established and applied to all systems development.

**Security in Application Systems Development (11.2.1.1)**

Input validation, authentication, and authorization should be included in the design, development and implementation of applications.

**Input and Data Validation (11.2.1.2)**

Applications should not pass raw input to other processes including, but not limited to, other applications, web services, application server and databases. Applications should use parameterized queries or stored procedures, not dynamic SQL statements.

**Output Data Validation (11.2.1.3)**

Applications should not echo input back to the user or disclose information about the underlying system through error messages.

**Application Authorization (11.2.1.4)**

Applications that provide access to information in databases or from network shares should perform user authentication.

**Inter-process Message Authentication (11.2.1.5)**

Inter-process message authentication should be used to verify that a message originated from a trusted source and that the message has not been altered during transmission.

**Control of Internal Processing (11.2.1.6)**

Security controls should be included to prevent corruption due to processing errors or deliberate acts.

**System Change Control Procedures (11.2.2)**

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

**Technical Review of Applications after Operating Platform Changes (11.2.3)**

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

**Restrictions or Changes to Software Packages (11.2.4)**

Modifications to software packages should be limited to necessary changes, and all changes should be strictly controlled.

**Secure System Engineering Principles (11.2.5)**

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

**Secure Development Environment (11.2.6)**

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

**Outsourced Development (11.2.7)**

Outsourced system development should be monitored and supervised to ensure the State's policies and practices are followed and to ensure appropriate security controls are in place.

**System Security Testing (11.2.8)**

Testing of security functionality should be carried out during development. Applications should be tested periodically throughout their respective lifecycles, at each major version release and prior to assigning public IP addresses or being moved or promoted into the production environment.

**System Acceptance Testing (11.2.9)**

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

**Test Data (11.3)**

Objective: To ensure the protection of the data used for testing.

**Protection of Test Data (11.3.1)**

Test data should be selected carefully, protected and controlled. The use of production data for development and testing is prohibited.

## 12. BUSINESS CONTINUITY MANAGEMENT

### **Information Business Continuity (12.1)**

Objective: To ensure the continued availability of business information and security enabled systems in the event of a crisis or disaster.

#### **Planning Information Systems Continuity (12.1.1)**

Teachstone should determine its requirements for information security and the continuity of information management systems in adverse situations, e.g. during a crisis or disaster.

#### **Implementing Information Systems Continuity (12.1.2)**

Teachstone should establish, document, implement and maintain processes, procedures and controls to ensure the required level of business continuity for all systems during an adverse situation.

#### **Verify, Review and Evaluate information Systems Continuity (12.1.3)**

All State agencies and vendors or contractors who operate on behalf of the State should verify the established and implemented information systems continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

### **Redundancies (12.2)**

Objective: To ensure availability of information processing facilities.

#### **Availability of Information Processing Facilities (12.2.1)**

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

## 13. INFORMATION SECURITY INCIDENT MANAGEMENT

### Management of Information Security Incidents and Improvements (13.1)

**Objective:** To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

#### Responsibilities and Procedures (13.1.1)

Teachstone will adhere to their Security Response Plan Policy as follows:

##### 1.1 Contact Information

The devops lead, Morgan Walker, 434-242-2456, and Director of Software Engineering and IT, Max Schubert, 434-825-7889, must be notified of any security-related incidents via phone call within 30 minutes of their detection.

##### 1.2 Triage

When an incident is detected, the on-call team shall:

Within 30 minutes of detection

- Notify the Director of Software Engineering and IT, the devops lead, and the software engineering lead of the incident

Within 2 hours of detection:

- Work together to determine the severity of the incident (impact and scope)
- Gather and store initial evidence of the incident as an incident in PagerDuty, utilizing as many people from the software engineering team as needed
- Identify next steps for action on the incident

##### 1.3 Mitigation and Remediation Timelines

After scope and severity are determined, the on-call team, working with the Director of Software Engineering and IT, shall determine mitigation and remediation. This includes:

Within 2 hours of detection

- Close off / Eliminate the points of entry used by attackers

Within 4 hours of detection

- Quarantine the affected systems if possible
- Scale up applications if capacity was reduced due to the loss of one or more server resources

Within 8 hours of detection

- If user data was compromised, inform the COO and work with the customer success team to determine which customers to notify and notify them

Within 16 hours of detection

- If used data was compromised or corrupted, determine if data restores are required from earlier backups, and restore data as needed. Prior to restore, snapshots of current data will be made for use in analysis and as evidence of the breach - within 16 hours of detection

## **Responsibilities and Procedures (13.1.1)**

### **Data Breach and Disclosure (13.1.2.1)**

Any State of Tennessee agency that discovers a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties must provide notice of the disclosure in accordance with TCA 47-18-2107 or any other applicable state and/or federal statute or regulations).Reporting Information

### **Security Weakness (13.1.3)**

Employees and contractors using Teachstone's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the Director of Software Engineering.

### **Assessment of and Decision on Information Security Events (13.1.4)**

Information security events should be assessed and a determination made on whether to classify the event as an incident in accordance with the Incident Response Plan.

### **Response to Information Security Incidents (13.1.5)**

Information security incidents will be managed in accordance with the documented procedures in Teachstone's Incident Response, Alerting and Communications Plan.

### **Learning from Information Security Incidents (13.1.6)**

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

### **Collection of Evidence (13.1.7)**

Teachstone should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

## 14. CRYPTOGRAPHY

### **Cryptographic Controls (14.1)**

Objective: To ensure proper and effective use of cryptography to protect the confidentiality and integrity of data owned or managed by the State. Confidential information must be encrypted by the use of valid encryption processes for data at rest and in motion as required by state or federal statute or regulation. This includes but is not limited to sensitive information stored on mobile devices, removable drives and laptop computers.

#### **Use of Cryptographic Controls (14.1.1)**

Cryptographic controls should be based on the classification and criticality of the data. In deciding what strength and type of control to be deployed, both stand alone and enterprise level encryption solutions should be considered. Attention should be given to regulations, national restrictions (e.g. export controls) that may apply to the use of cryptographic techniques.

#### **Transmission Integrity (14.1.2)**

Information systems should protect the integrity of transmitted information traveling across both internal and external communications. This control applies to communications across internal and external networks

#### **Transmission Confidentiality (14.1.3)**

Information systems should protect the confidentiality of transmitted information. Teachstone will employ mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

#### **Cryptographic Module Authentication (14.1.4)**

Information systems must use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal statutes, state statutes, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. The list of cryptographic modules in use will be compared to the list of NIST validated cryptographic modules quarterly to ensure compliance.

#### **Cryptographic Module Authentication (14.1.5)**

Information systems will obtain and issue public key and Transport Layer Security (TLS) certificates from an approved service provider. This control focuses certificates with visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services. Secure Socket Layer (SSL) protocol must be disabled on all devices.

### **Key Management (14.1.6)**

A secured environment should be established to protect the cryptographic keys used to encrypt and decrypt information. Cryptographic key management and establishment will be performed using automated mechanisms with supporting manual procedures. Keys should be securely distributed and stored. Access to keys should be restricted only to individuals who have a business need to access them. All access to cryptographic keys requires authorization and should be documented. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

## 15. COMPLIANCE

### **Compliance with Legal and Contractual Requirements (15.1)**

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations] related to information security and of any security requirements.

#### **Identification of Applicable Legislation and Contractual Requirements (15.1.1)**

All relevant legislative, statutory, regulatory, contractual requirements and Teachstone's approach to meet these requirements should be explicitly identified, documented and kept current for each information system and each entity that stores, processes or transmits data on behalf of Teachstone.

#### **Intellectual Property Rights (15.1.2)**

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products.

#### **Protection of Records (15.1.3)**

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with state or federal statutory, regulatory, contractual and business requirements.

#### **Privacy and Protection of Personally Identifiable Information (15.1.4)**

The privacy and protection of personally identifiable information should be ensured as required by relevant federal or state statute or regulation.

#### **Regulation of Cryptographic Controls (15.1.5)**

Cryptographic controls should be used in compliance with state or federal statutory, regulatory, contractual and business requirements.

### **Information Security Reviews (15.2)**

Objective: To ensure that information security is implemented and operated in accordance the organizational policies and procedures.

### **Independent Review of Information Security (15.2.1)**

The State's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently and at planned intervals or when significant changes occur.

### **Compliance with Security Policies and Standards (15.2.2)**

Managers should regularly review the compliance of information processing and procedures within their area of responsibility for accuracy and applicability with the appropriate security policies, standards and any other security requirements.

### **Technical Compliance Review (15.2.3)**

Information systems should be regularly reviewed for compliance with Teachstone's information security policies and standards.

## 16. HUMAN RESOURCE

### **Prior to Employment (16.1)**

Objective: To ensure all full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors understand their responsibilities in regards to information security requirements for the State of Tennessee's computing environments.

#### **Screening (16.1.1)**

Background and verification checks on all candidates for employment should be conducted in accordance with relevant statutes and published state policies.

#### **Acceptable Use Policy (16.1.2)**

Teachstone shall ensure that their full- and part-time employees and all third parties, contractors, or vendors who use Teachstone resources have read and accept the terms of Teachstone's Employment Policies. Proof of employee acceptance and acknowledgement will be maintained by Teachstone.

### **During Employment (16.2)**

Objective: To ensure employees and contractors are aware of and fulfill their information security responsibilities.

#### **Management Responsibilities (16.2.1)**

Management should ensure that all employees and contractors are aware of and fulfill their information security responsibilities.

## 17. VERSION HISTORY

Version 2.1 – December 15, 2016	<i>Converted Office for Information Resources to Strategic Technology Solutions. Updated policy link in 2.4 Made agency specific policies mandatory for agency specific requirements in 3.1.2. Minor wording changes to sections 13.1.1 and 13.1.2. Updated technology requirement for encryption in 14.1.5. Aligned training periodicity with ISC vote in 16.2.2.</i>
---------------------------------	--

## 18. TERMS AND DEFINITIONS

**Access Credentials** - Access Credentials are issued to users to provide access to particular data or resources. Examples include passwords, badges, and card keys for doors.

**Access Granting Authority** – The access granting authority is the individual or group that has the responsibility for determining appropriate access and use of resources.

**Asset** – An asset is anything that can be considered a resource such as employees, computer hardware, computer software, and data.

**Authentication** – Authentication is the process of ensuring an individual is who they claim to be.

**Authorization** – Authorization is the process of providing permission to access resources or to perform operations.

**Business Continuity** – Business Continuity is the ability of an organization to continue its operations and services in the face of a disruptive event.

**Business Impact Analysis (BIA)** – A Business Impact Analysis is a process that is performed to identify and evaluate the potential impacts of natural and manmade events on business operations.

**Cloud Computing** – Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

**Confidential Data** – is a generalized term that typically represents data classified as Confidential as defined by state or federal statute, regulation or as defined by the Payment Card Industry.

**Cryptography** - Cryptography is the science of transforming information into a secure form so that it can be transmitted or stored, and unauthorized persons cannot access it.

**Custodian** – Custodian is the individual or group that is responsible for granting access to data and or network resources.

**Data Classification** – Data Classification is the process of identifying the levels of protection mechanisms and restrictive access that are required for data based on state or federal statute, regulation and/or criticality and of the data.

**Data Validation** – Data validation is the process of ensuring that a program operates on clean, correct and useful data.

**Hash** – A hash is a cryptographic algorithm that can later be decrypted. It is frequently used for comparison purposes to validate the integrity of the data.

**Information Systems Council (ISC)** – The Information Systems Council is legislatively mandated to provide high level oversight and direction for State of Tennessee information systems and processing.

**Input Validation** – Input validation is a type of data validation that is applied to data from untrusted sources.

**Least Privilege** – Least Privilege is a practice where the minimum level of access or privileges required to perform an individual's job duties are granted.

**Logic Bomb** – A logic bomb is computer code that lies dormant until it is triggered by a specific logical event.

**Mobile Device** – A mobile device is a computing platform that not meant to be stationary. Examples include but are not limited to laptops, tablets, i-Phones, i-Pads and android devices.

**Multifactor Authentication** – Multifactor Authentication is using more than one factor to authenticate an individual or resource. Factors include something you know (password), something you have (token or smartcard) and something you are (biometrics such as iris or retinal scans or fingerprints).

**Owner** – Owner is the individual who is the final authority and decision maker in determining how data and resources are used in State business and what level of access will be granted to them.

**Payment Card Industry (PCI)** – The Payment Card Industry is comprised of the organizations that transmit, process or store cardholder data. The PCI works with the Payment Card Industry Security Standards Council to develop Payment Card Industry Data Security Standards.

**Rootkit** – A rootkit is a set of software tools used by an attacker to hide the actions or presence of other types of malicious software.

**Salt** - A salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase, making the stored data more difficult to crack.

**Security Advisory Council** – The Security Advisory Council is comprised of the directors in Strategic Technology Solutions.

**Security Event** – A security event is an event that adversely impacts the established security behavior of an environment or system

**Security Incident** - A security incident can be accidental or malicious actions or events that have the potential of causing unwanted effects on the confidentiality, integrity and availability of State information and IT assets.

**Service Account** – A service account is an account that is used by systems, services or applications, not by individuals. **Trojan Horse** – A trojan horse (or Trojan) is an executable program advertised as performing one activity, but actually does something else.

**Virtual Private Network (VPN)** – A VPN extends a private network across a public network, such as the Internet. It enables a computer or wireless enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

**Virus** – A computer virus is malicious computer code that reproduces itself on the same computer.

**Worm** – A computer worm is a malicious program that takes advantage of a vulnerability on one computer and spreads itself to other computers with the same vulnerability.

**19. APPENDICES**

- Appendix A State of Tennessee Approved Login Banner
- Appendix B Secure Application Development
- Appendix C Information Security Incident Response and Alerting Communications Plan

# Enterprise Information Security Policies

Administration      State of Tennessee Department of Finance and  
Strategic Technology  
Solutions

Document Version 2.1

December 15, 2016



Mark Bengel CIO



Curtis Clan,  
CISO

Client#: 1621577

44TEACHTRA

**ACORD**

**CERTIFICATE OF LIABILITY INSURANCE**

DATE (MM/DD/YYYY)

11/08/2017

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> <b>BB&amp;T Insurance Services, Inc.</b> 1425 Seminole Trall, 2nd Floor Charlottesville, VA 22901 434 979-7064		<b>CONTACT NAME:</b> <b>PHONE (A/C, No, Ext):</b> 434 979-7064 <b>FAX (A/C, No):</b> 888 632-8470 <b>E-MAIL ADDRESS:</b>	
<b>INSURED</b> <b>Teachstone Training LLC</b> 675 Peter Jefferson Parkway, Suite 400 Charlottesville, VA 22911		<b>INSURER(S) AFFORDING COVERAGE</b> <b>INSURER A:</b> Massachusetts Bay Ins. Co. <b>NAIC #</b> 22306 <b>INSURER B:</b> <b>INSURER C:</b> <b>INSURER D:</b> <b>INSURER E:</b> <b>INSURER F:</b>	

**COVERAGES** **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL SUBR INSR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> <b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:		UODR518147810	01/31/2017	01/31/2018	EACH OCCURRENCE \$1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$300,000 MED EXP (Any one person) \$5,000 PERSONAL & ADV INJURY \$1,000,000 GENERAL AGGREGATE \$2,000,000 PRODUCTS - COMP/OP AGG \$2,000,000 \$
A	<b>AUTOMOBILE LIABILITY</b> <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS		UODR518147810	01/31/2017	01/31/2018	COMBINED SINGLE LIMIT (Ea accident) \$1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input checked="" type="checkbox"/> <b>UMBRELLA LIAB</b> <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$0		UODR518147810	01/31/2017	01/31/2018	EACH OCCURRENCE \$10,000,000 AGGREGATE \$10,000,000 \$
A	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N N/A	WDR984354904	01/31/2017	01/31/2018	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$1,000,000 E.L. DISEASE - EA EMPLOYEE \$1,000,000 E.L. DISEASE - POLICY LIMIT \$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

**CERTIFICATE HOLDER**

**CANCELLATION**

The State of Tennessee CPO Risk Manager 312 Rosa L Parks Ave 3rd Floor Central Procurement Office Nashville, TN 37243	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.  AUTHORIZED REPRESENTATIVE <i>Byron P. Barton, Jr.</i>
---	--

# Amendment Request

This request form is not required for amendments to grant contracts. Route a completed request, as one file in PDF format, via e-mail attachment sent to: [Agsprrs.Agsprsr@tn.gov](mailto:Agsprrs.Agsprsr@tn.gov)

<p><b>APPROVED</b>  <b>Michael F. Perry,</b>  <b>Chief Procurement</b>  <b>Officer by T. L. Stuart</b>  <b>CPO Attorney</b></p>	<p>Digitally signed by Michael F. Perry, Chief Procurement Officer by T. L. Stuart CPO Attorney                  DN: cn=Michael F. Perry, Chief Procurement Officer by T. L. Stuart CPO Attorney, o=Central Procurement Office, ou=DGS, email=toni.stuart@tn.gov, c=US                  Date: 2018.05.11 14:27:28 -05'00'</p>
<b>CHIEF PROCUREMENT OFFICER</b>	<b>DATE</b>

<b>Agency request tracking #</b>	33132-00317
<b>1. Procuring Agency</b>	TN Dept. of Education (TDOE)
<b>2. Contractor</b>	Teachstone Training, LLC
<b>3. Edison contract ID #</b>	56904
<b>4. Proposed amendment #</b>	01
<b>5. Contract's Original Effective Date</b>	January 19, 2018
<b>6. Current end date</b>	January 18, 2019
<b>7. Proposed end date</b>	January 18, 2019
<b>8. Current Maximum Liability or Estimated Liability</b>	\$ 190,850.00
<b>9. Proposed Maximum Liability or Estimated Liability</b>	\$ 895,812.00
<b>10. Strategic Technology Solutions Pre-Approval Endorsement Request</b> – information technology service (N/A to THDA)	<input type="checkbox"/> Not Applicable <input checked="" type="checkbox"/> Attached
<b>11. eHealth Pre-Approval Endorsement Request</b> – health-related professional, pharmaceutical, laboratory, or imaging	<input checked="" type="checkbox"/> Not Applicable <input type="checkbox"/> Attached
<b>12. Human Resources Pre-Approval Endorsement Request</b> – state employee training service	<input checked="" type="checkbox"/> Not Applicable <input type="checkbox"/> Attached
<b>13. Explain why the proposed amendment is needed</b>	
An amendment is needed to add the renewal clause, update scope to expand observation pilot to include all VPK and PDG classrooms across the state, increase maximum liability and update payment methodology.	
<b>14. If the amendment involves a change in Scope, describe efforts to identify reasonable, competitive, procurement alternatives to amending the contract.</b>	
The contractor is currently working on a pilot of data collection for voluntary pre-K (VPK) program quality monitoring and professional development, and the TDOE needs to expand this work to the	

<b>Agency request tracking #</b>	33132-00317
<p>remaining 789 VPK classrooms throughout the state. This is needed to support the TDOE's work under the Pre-K Quality Act of 2016, which requires the Office of Early Learning to work toward improving the consistency of quality in pre-K classrooms across the state. To accomplish this work, we must gather data regarding current program quality practices. Alternative procurement options are not available for this work, as the contractor is the sole provider of the CLASS system, the only system that supplies analysis of teacher-student interactions in the pre-K classroom.</p>	
<p><b>Signature of Agency head or authorized designee, title of signatory, and date</b> (the authorized designee may sign his or her own name if indicated on the Signature Certification and Authorization document)</p> <p><b>Candice McQueen_jc</b> Digitally signed by Candice McQueen_jc DN: cn=Candice McQueen_jc, o, ou=TN Department of Education, email=joanna.collins@tn.gov, c=US Date: 2018.05.11 12:57:07 -05'00'</p>	



## CONTRACT AMENDMENT COVER SHEET

<b>Agency Tracking #</b> 33132-01118	<b>Edison ID</b>	<b>Contract #</b> 56904	<b>Amendment #</b> 01		
<b>Contractor Legal Entity Name</b> TEACHSTONE TRAINING, LLC			<b>Edison Vendor ID</b> 0000206628		
<b>Amendment Purpose &amp; Effect(s)</b> Add renewal clause, expand observation pilot to include all VPK and PDG classrooms across the state, increase maximum liability, and update payment methodology					
<b>Amendment Changes Contract End Date:</b> <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		<b>End Date:</b> January 18, 2019			
<b>TOTAL Contract Amount INCREASE or DECREASE per this Amendment</b> (zero if N/A):			<b>+ \$ 704,962.00</b>		
<b>Funding —</b>					
<b>FY</b>	<b>State</b>	<b>Federal</b>	<b>Interdepartmental</b>	<b>Other</b>	<b>TOTAL Contract Amount</b>
2018	\$190,850.00				\$190,850.00
2019		\$589,870.00			\$589,870.00
2019	\$115,092.00				\$115,092.00
<b>TOTAL:</b>					<b>\$895,812.00</b>
<b>American Recovery and Reinvestment Act (ARRA) Funding:</b> <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO					
<b>Budget Officer Confirmation:</b> There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.				<i>CPO USE</i>	
<b>Speed Chart</b> (optional)			<b>Account Code</b> (optional)		

**AMENDMENT 01  
OF CONTRACT 56904**

This Amendment is made and entered by and between the State of Tennessee, Department of Education, hereinafter referred to as the "State" and Teachstone Training LLC, hereinafter referred to as the "Contractor." For good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually understood and agreed by and between said, undersigned contracting parties that the subject contract is hereby amended as follows:

1. Contract section A.3. is deleted in its entirety and replaced with the following:

A.3. Using the CLASS evaluation system, the Contractor shall conduct in-person observations of student/teacher interactions in up to 989 Tennessee Voluntary Pre-K (VPK) classrooms, designated by OEL, and provide feedback and reports to the State. This shall include at minimum:

a. Observations shall have a specific focus on emotional support, classroom organization and instructional support, and all of their subcategories as listed in the CLASS Dimensions Guide.

b. The Contractor shall complete 1 four cycle observation of each classroom, up to two hundred (200), within the first ninety (90) days of the Effective Date. The Contractor shall complete one (1) four (4) cycle observation of each classroom, up to seven hundred and eighty-nine (789), between September 4, 2018 and December 10, 2018. For these purposes, a four (4) cycle observation takes place over a two (2) hour time period (consisting of four (4) thirty (30) minute cycles) and includes snapshots of interactions at four (4) different points during that period.

c. The Contractor shall provide data reports to the State in the myTeachstone system including the in-person rating of the classroom quality using the CLASS evaluation system. Data reports shall include classroom, school, district, and State level data and not contain student personally identifiable information. The State shall have access to every Pilot Participant's data. The Contractor shall also provide a final report to the State that includes all raw data collected pursuant to this Contract.

d. If requested by the State, the Contractor shall provide reports on student-teacher interactions, as rated during the classroom observations, to OEL, school administrators and district coaches. Reports shall include all metrics evaluated by the CLASS evaluation system. School administrators and district coaches shall have access to feedback and reports related to their own classrooms, schools, and districts and will not have access to other Pilot Participants' data.

e. All data gathered by the Contractor shall not be shared with third parties (including districts, teachers, and coaches) unless approved by the State. This pre-approval requirement also applies to providing districts with individual reports regarding teacher performance.

2. Contract section A.5. is deleted in its entirety and replaced with the following:

A.5. If requested by the State and once staff are trained to observe, the Contractor shall provide TTT observer training to no less than two (2) members OEL staff (could be additional attendees) within the first six (6) months of the Contract. The TTT observer training covers training others to use the CLASS evaluation system and its rating scales and data analysis. TTT Trainees may subsequently train an unlimited number of State employees and a maximum of fifteen (15) district level observers during the term of this Contract. There is no limit on the number of Introduction to CLASS trainings that TTT Trainees may conduct.

a. The Contractor shall provide all Materials associated with TTT training, including: Participant guides for the Intro and Obs training, Facilitator guides for the Intro and Obs training, DVD/or flash drive of videos, participant guide for the TTT session, one dimension guide, one score sheet, an exemplar video description booklet, one year access to the Pre-K video library, (when completing training) access to the Affiliate Trainer Panel (this is where the PowerPoints and other

affiliate resources are), and a master code justification. The printed Materials should come in a big binder with tabs. One copy of the TTT training Materials shall be provided for each attendee.

3. Contract section A.9. is deleted in its entirety and replaced with the following:
  - A.9. If requested by the State, the Contractor shall provide eight (8) on-site, full-day trainings for up to fifty (50) teachers participating in the observations. These trainings will provide an overview of the CLASS evaluation tool including what is measured, how it is measured, and how to change practice as a result of the measurements.
    - a. If requested by the State, the Contractor shall provide copies of Materials so that the State trainers can conduct the trainings in-house. Materials include the CLASS Dimensions Guide and associated Materials.
4. The following is added as Contract section A.14 and all subsequent sections are renumbered accordingly.
  - A.14. Project management and reporting fee. The Contractor shall provide project management services in fulfilling the timely and efficient completion of live observations for up to 789 classrooms, contingent on completion of deliverables as described in section C.3. Project management services are including, but not limited to: scheduling, logistics, coordination, and project reporting.
5. Contract section B. is deleted in its entirety and replaced with the following:
  - B. TERM OF CONTRACT:**
    - B.1. This Contract shall be effective for the period beginning on January 19, 2018 ("Effective Date") and ending on January 18, 2019 ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.
    - B.2. Renewal Options. This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to two (2) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.
    - B.3. Term Extension. The State may extend the Term an additional period of time, not to exceed one hundred-eighty (180) days beyond the expiration date of this Contract, under the same terms and conditions, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.
6. Contract section C.1. is deleted in its entirety and replaced with the following:
  - C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed eight hundred ninety-five thousand eight hundred twelve dollars and zero cents (\$895,812) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.
7. Contract section C.3. is deleted in its entirety and replaced with the following:
  - C.3. Payment Methodology. The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.

a. The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.

b. The Contractor shall be compensated based upon the following payment methodology:

<b>Goods or Services Description</b>	<b>Amount (per compensable increment)</b>
A.3. Live observation of up to two hundred (200) classrooms and provision of feedback and reports (spring 2018)	\$100,000 total (\$500 per four cycle CLASS observation classroom evaluation)
A.3. Live observation of up to seven hundred and eighty-nine (789) new classrooms and provision of feedback and reports (fall 2018), contingent on completion of deliverable as described below: <ul style="list-style-type: none"> <li>• Documentation for all observations which are not held at a rate of two per day to include reason for deviance from observation schedule plan referenced in A.14.</li> </ul>	\$615,420 maximum total (\$1,300 per day at two (2) observations completed per day for 80% of the time over sixty-five (65) days)
A.4. Initial observer training for OEL staff	\$900 per staff member that receives training
A.5. TTT training for no less than two members of OEL staff, including all Materials	\$4,700 per staff member that receives training
A.6. up to two hundred (200) subscriptions to myTeachstone	Up to \$22,000 total (\$110 per subscription - per subscription cost includes start-up fee)
A.7. On-site training for 21 leaders and 5 OEL staff Coaching with myTeachstone. This is a 2 day (16 hour) training session.	Up to \$12,500 total; \$8,500 for the first fifteen (15) participants and \$350 for each additional participant.
A.8. Monthly support calls or webinars with coaching specialist, up to 10 calls	\$150 per call
A.9. Completion of 1 day (8 hour) on-site introduction to CLASS tool, for teachers (50 members)	\$7,000 per session
A.9(a). Materials for State trainers to provide training in-house	\$75 per copy of materials
A.10. CLASS observation training, two (2) two (2) day (sixteen (16) hours total) sessions, including Materials	\$8,500 per session
A.14. Project management and reporting fee, contingent on completion of deliverable as described below <ul style="list-style-type: none"> <li>• Observation schedule plan provided to OEL for all seven hundred and eighty-nine (789) observations, to include a minimum of one (1) contingency observation site and documented attempt to schedule all observations at a minimum rate of two (2) per day within thirty (30) days of fully executed contract and no later than August 10, 2018</li> </ul>	\$61,542.00 maximum total [10% of completed live coding cost for fall 2018 observations (up to seven hundred and eighty-nine (789))]

Required Approvals. The State is not bound by this Amendment until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).

Amendment Effective Date. The revisions set forth herein shall be effective July 15, 2018. All other terms and conditions of this Contract not expressly amended herein shall remain in full force and effect.

**IN WITNESS WHEREOF,**

**TEACHSTONE TRAINING LLC:**

---

**SIGNATURE**

**DATE**

---

**PRINTED NAME AND TITLE OF SIGNATORY (above)**

**DEPARTMENT OF EDUCATION:**

---

**CANDICE MCQUEEN, COMMISSIONER**

**DATE**