	Technology Services Performance Excellence and Customer Care Center	**SOP #**	TS -PE-535
		Revision #	
		Implementation Date	09/01/14
Page #	1 of 2	**Last Reviewed/Update**	09/01/18
SOP Owner	Jennifer Miller	**Approval**	Jennifer Miller
SOP Name	Software and Application Purchase/Utilization Procedure		

Standard Operating Procedure

1. Purpose

The purpose of this procedure is to document the process to utilize software, applications and/or web services on district computers.

2. Scope

This procedure is intended for all digital resource requests.

3. Prerequisites

Curriculum approval is required for any student/teacher digital resource utilization.

DII approval is required for any administrative software installation.

4. Responsibilities

It is the responsibility of Technology Services to ensure the process is completed.

5. Process

#	Step	Responsibility
1	Teacher or Curriculum Coordinator will request digital resource through the iSupport system.	Teacher/Coordinator
2	Request will include the following information: name of resource, website link to resource (if applicable), cost, payment responsibility, budget code, principal, grade level for use, content area for use, media release requirements, TEKS addressed, student use vision, Common Core alignment, student login requirement, student data shared.	Teacher/Coordinator
3	Request will be assigned to the Cybersecurity team to begin security vetting process.	CCC Team
4	Cybersecurity team will evaluate resource's privacy policy. If student data is required for resource, a student Data Privacy Agreement (DPA) will be sent to vendor. Cybersecurity team will work with the vendor to answer questions as needed.	CCS Team
5	If requested resource is a website, or requires the use of a website, Cybersecurity team will use Qualys SSL Server Test to verify the website is secure. If substandard grade is scored, cybersecurity team will notify vendor to improve SSL Grade.	CCS Team

6	Security vetting completion is dependent upon receipt of a signed DPA (if student data is required) for resource, and an SSL server grade of A or better (if resource utilizes a website). If all conditions are met, or determined to not apply, process continues to step 7. If conditions are not met, request will be denied, and process will end. Cybersecurity team will upload status of resource as **Not Approved** to TXSPA Database for staff access and transparency.	CCS team
7	If security standards are met during vetting process, resource request will be assigned to Instructional Technology team for curriculum approval or assigned to DII team for administrative approval.	Instructional Technology/DII team
8	Curriculum team will review the software/application/web service for use in the classroom.	Instructional Technology
9	If resource does not align with the curriculum focus, request will be denied, and process will end.	Instructional Technology
10	If the resource is approved by curriculum, the iSupport request will be escalated to the DII to verify resource is technically sound with district devices.	Instructional Technology
11	If requested resource is not technically sound, DII will work with the Instructional Technology team to obtain a replacement. The security vetting process will begin again at step 4 after replacement found.	DII Team/CCS Team
12	If resource is technically sound and approval has been given by curriculum, then the iSupport request is escalated to the AAS team. If resource is free, proceed to step 15.	DII Team
13	AAS team will request quote(s) from vendors and issue PO.	AAS Team
14	If the request is software, the software will be delivered to AAS and the license(s) will be stored for compliance.	AAS Team
15	Resource will be installed on requested setup(s).	DII Team
16	Cybersecurity team will upload status of resource as **Active / Approved** to TXSPA Database for staff transparency.	CCS Team
17	Data Privacy Agreement and SSL grade will be renewed annually if applicable.	CCS Team