Technology Acquisition Review Process

Overview

Stanislaus State technology acquisitions, whether purchased or obtained at no cost - including free software, are to be reviewed for Enterprise Support, Accessibility and Information Security compliance prior to acquisition. The Technology Acquisition Review Process (TAR Process) has been established to conduct product reviews that will be used to determine the level of support required from the Office of Information Technology for the following:

- Support and service models;
- Potential integrations that may be needed with other systems or data;
- To establish if there is existing similar technology already in use on campus to prevent redundant costs;
- IT process alignment;
- Any timing or scheduling constraints.

Technology acquisition reviews (TARs) are also to be used to:

- Reduce IT costs;
- Meet compliance requirements with CSU policies and Stanislaus State practice directives for data and system protection and accessibility; and
- Reduce the risk of data breaches resulting in: harm to CSU; individuals or intellectual property rights; and any associated legal/reputational penalties.

TAR Process.

Process Steps:

1. Check the authorized list and use authorized technology where possible.
2. The Stanislaus State faculty or staff member who is most knowledgeable about the technology should be the individual who completes and submits the TAR form in Team Dynamix. Assistance from Office of Information Technology support staff may be requested if necessary. The more detailed information received, the quicker the review can be completed.
3. TAR Process requests will be tracked using service request tickets created in Team Dynamix.
    - Requestor provides requested documentation and responds to additional questions.
    - Office of Information Technology teams will review the request to determine support and service level models needed, integrations, and IT process alignment, and to reduce potential redundant technology and any timing constraints. This will be the first level of review and approval is needed before the request is submitted for security/privacy or accessibility reviews.
    - Information Security team members determine if supplemental IT contractual terms are needed.
    - Accessible Technology team members determine compliance with ATI policy.
    - TAR Requests will be updated to indicate if the requested technology has been approved or not approved.

4. Requesting department must provide the approved TAR Request number and documentation to Procurement & Contract Services when submitting their purchase request.

NOTE:

Timeline for TAR and Purchasing Process

The timeline to complete a TAR review is estimated at a minimum of 10 business days. Complex review cases or cases that require the involvement of legal may require additional time to review. TAR reviews should be requested in advance to minimize delays in the procurement process. The completion of the TAR review is a pre-requisite of the procurement process and the timeline does not include the time required by Procurement & Contract Services to complete the purchase. If your proposed technology or service involves any of the following components, please reach out to the respective business areas and obtain written approval from them, which should then be submitted with the TAR Request. This will help us process your request faster.

1. Any TAR that collects money requires the approval of Financial Services.
2. Any TAR that involves marketing, branding, advertising, and social media needs approval from Communications and Public Affairs.

Compliance

TARs are required to ensure compliance with CSU policy and Stanislaus State practice directives for data and system protection, and to reduce the risk of data breaches resulting in: harm to CSU, individuals or intellectual property rights; and any associated legal/reputational penalties.

Deployment Requirements

All technology must be deployed in a manner that meets the following requirements. Enterprise Support, Information Security and Accessibility reviews may identify additional requirements as applicable.

1. Networked devices must meet CSU Common Network Infrastructure (CNI) standards.
2. Use in-transit and at-rest encryption for all sensitive data.
3. Authorization and access control must be managed for all sensitive data and in accordance with existing centralized identity and access management methods where possible (configured to use Stanislaus State's single sign-on).
4. The business reason for storing any confidential data must be documented, and a data retention schedule must be established and followed (e.g., how long the data will be kept, how it will be destroyed, etc.).
5. Maintain university ownership by using Stanislaus State credentials to register and manage Cloud/Internet service accounts.
6. Install security updates and patches provided by the manufacturer as soon as reasonable, based on severity (and after adequate testing).
7. Meet requirements of Accessible Technology Initiative.
8. Do not store or transmit protected University data using services hosted by third parties which do not have a contract in place with the campus or its Auxiliaries, such as personal cloud accounts.
9. Do not sign up for or accept terms of service/use for a cloud service without first obtaining prior approval from Procurement & Contract Services, even if the service is no cost.

- Integrated California State University Administrative Manual (ICSUAM)
    - Section 8000 - Information Security
        - 8040 Managing Third Parties
        - 8055 Change Control
        - 8060 Access Control
        - 8065 Asset Management
        - 8075 Information Security Incident Management
        - 8085 Business Continuity and Disaster Recovery
    - Section 5000 - Contracts and Procurement
- CSU Accessible Technology Initiative (ATI)
- Stanislaus State Practice Directives
    - Information Technology
        - Confidential Data
        - Cloud Computing
        - Credit Card Payment Processing and PCI Security
        - Logging and Threat Management
        - Password
    - Financial Services
        - Procurement Cards

Authorized Technology

Authorized technology does not require a TAR. Authorized technologies are low risk or have already completed Enterprise, Information Security and Accessible Technology Team reviews. The list below has been approved and will be reviewed and updated frequently. All updates to the list can be found at the Accessible Technology Website.

Web applications and cloud services

Authorized campus standard cloud technology should be used where it provides equivalent functionality. Exception requests to use a non-standard cloud technology require a documented business reason why the campus provided standard technology cannot be used, and should be documented in the TAR. The cloud computing services listed below have been authorized:

- Box cloud storage - (replaces DropBox, iCloud, Amazon, Google drive)
- Qualtrics survey platform - replaces SurveyMonkey and WuFoo)
- Zoom videoconferencing - (replaces GoToMeeting)

- Online instruction used by fewer than 20 employees
    - Microsoft Office 365 Online (browser based) – Word, Excel, PowerPoint, Teams
        - Available on request only: Forms, Planner, Project, Power BI, and Flow
    - Twitter
    - LinkedIn
    - Indeed
    - ServiceNow

Digital content

Copyrighted information assets purchased for Stanislaus State use, such as:

- Fonts
- Images
- Music
- Photographs
- Text-based information/data
- Video-based information/data

Each purchaser is responsible for retaining proof of sale and/or licensing agreement information associated with the purchase of copyrighted materials for as long as the digital content is used/stored.

Software

Contact the Office of Information Technology Support Desk to obtain the following software at low or no cost:

- Adobe (Acrobat DC Pro, Photoshop, and other tools)
- Dragon Dictate and Naturally Speaking
- Mathematica
- Matlab
- McAfee Anti-virus software
- Microsoft Office 365 (full client) - (Access, Excel, Outlook, PowerPoint, Publisher, Word, Defender)
- Microsoft Project
- Microsoft Visio
- Microsoft Windows Operating System / MacOS
- Minitab
- Qualtrics
- SAS

- SPSS

Hardware, equipment, and supplies

For tablets, laptops, and desktop computers - see Apple and Dell listings in CSUBUY. Acquisition of 20 or more computers or tablets requires a TAR and Procurement involvement in order to complete.

- Adapters
- Batteries
- Cables
- Cameras and video cameras (does not include security, monitoring, or surveillance cameras) (refer to Confidential Data Policies/Practices and Guidelines)
- Compact Disks and tapes (refer to Confidential Data Policies/Practices and Guidelines)
- Digital voice recorders (refer to Confidential Data Policies/Practices and Guidelines)
- Displays
- Docking Stations
- DVD players/Blu-Ray players
- Hard drives (refer to Confidential Data Policies/Practices and Guidelines)
- Headphones and headsets
- Input devices (e.g. mice, trackballs, track pads, Apple Pencils, Microsoft Pens and keyboards)
- Label maker/ label printer - Brother
- Memory (RAM)
- Monitors – aligned with campus standards, current model is: Dell Ultra sharp 24
- Network equipment peripherals, such as: cables, port adapters, stand-alone power supplies (not network connected)
- Port replicators
- Scanners
- Smart TVs - Samsung brand. These may not be connected to the Stanislaus State network. Installation of equipment purchased must be managed as part of an authorized project.
- Sound cards
- Speakers
- Televisions without Wi-Fi, Internet, or network connections
- Uninterruptible Power Supplies (UPS)

- USB drives (Note: these are not approved for storing Level 1 and Level 2 data. Special encrypted flash drives are required, along with approved procedures for proper management. Reach out to Office of Information Technology Support for more guidance.)
- USB hubs
- Video cards
- Printers used to print Level 1 or Level 2 data require a TAR

Tablets, laptops, and desktop computers – the below items are available for purchase in CSUBUY but they are **not** authorized for storing Level 1 data without additional security controls. If in doubt whether or not Level 1 data may be involved, please submit a TAR Request.

- Apple iPad and iPod
- Apple MacBook, MacBook Pro, MacBook Air, iMac
- Dell Latitude 7000, Precision 5000, Optiplex 7000

Maintenance and Renewals

TAR reviews will be completed every three years for authorized technology products that are for maintenance purposes or are a renewal where:

1. The scope of deployment and the technology and/or technology services have not changed.
2. There are no changes to functionality or capabilities, regardless of whether they are turned on or not.
3. Replacement parts are the same or similar to the part being replaced.

It is necessary to provide Procurement & Contract Services with the original approved TAR service request number. If you need help locating a previously-approved TAR, please reach out to the Office of Information Technology Support Desk.

Mandatory Technology Reviews

TAR reviews are always required for the following items:

1. Drones
2. Domain Registration Services (initial requests and renewals) – this is for tracking and compliance reasons.

Frequently Asked Questions

Is a review needed?

Is a review needed if another campus unit has an approved TAR?

Yes, a review is needed even if another department has an approved TAR, unless the product or service is on the authorized list. Adding more users may change the support model, accessibility impact, and/or security risk. Prior reviews can expedite new TAR reviews. Please reference the previously approved TAR in the notes section of the form. Technology acquired by more than one unit is considered for campus-wide acquisition and pre-approval.

Is a review needed if the technology is already used at another CSU campus or has an existing system-wide agreement?

Yes, a review is needed even if another CSU campus has already acquired the technology. Enterprise. Information Security and Accessibility reviews copies of contracts from other campuses to help expedite TAR reviews. Submit the TAR form with any supporting documentation you have, such as: emails, another campus' Higher Education Cloud Vendor Assessment Tool (HECVAT), links to CSUBUY Contract Store documents, and copies of contracts. By providing as much detail and support possible, it is possible that these will help expedite TAR reviews.

Is a review needed if I am the only user of the technology?

Yes, a review is needed even if used by one employee, unless it's for online instruction of 20 or fewer employees. Technology that stores or processes sensitive data or connects to the campus network may impact other software on laptops/desktop computers or could have a security risk. Technology used to create or manage information can introduce accessibility barriers for other individuals. In addition, the TAR process helps centrally collect and manage the campus software and services inventory to demonstrate compliance with software licensing requirements. Technology acquired by more than one unit is considered for campus-wide acquisition and pre-approval.

Is a review needed for Qualtrics Panels?

No, a TAR is not needed for Qualtrics Panels. Acquisition of these services should be coordinated with Procurement & Contract Services.

What if there are changes to scope or nature of deployment following review?

If the scope or nature of deployment changes, please submit another TAR Form. An example of scope change is expanding the technology to more users. An example of the nature of deployment changing is changing a workflow to collect confidential data elements that weren't being collected previously.

Can I buy software using my campus procurement card?

Software that is not under an existing campus or systemwide agreement or that has not been authorized via the campus TAR Process cannot be purchased on a campus procurement card. All software purchases must complete the review process and receive authorization from Office of Information Technology and Procurement & Contract Services prior to a completed purchase. Only software that is under an existing agreement or has received authorization from Office of Information Technology and Procurement & Contract Services can be procured on a campus procurement card.

Do I need a TAR for Online Instruction/Virtual Event?

A TAR is NOT required for internal events held using Zoom or Teams. Please follow accessibility guidance for these events.

A TAR will not be required when Stan State employees attend training (in person or online), professional development events or online conferences/events, including payment of associated registration fees.

A TAR is still required when a third-party instructional course or platform is used by students.

Completing the form

Who should complete the form?

The requestor (contact) should be the Stanislaus State faculty or staff member who is most knowledgeable about the technology being reviewed. Some of the questions are technical and may require consulting the Vendor or Office of Information Technology support.

How can I get help completing the form?

Contact the Office of Information Technology Support Desk to request assistance completing the TAR form.

What do I do if I don't know the answer to a question on the form?

All questions must be answered accurately before a review can be completed. If a question is not answered, the highest possible risk will be assumed. Contact the Vendor or Office of Information Technology Support Desk to obtain assistance completing the TAR form.

How do I see my tickets?

Visit and log into Team Dynamix using your Stanislaus State ID and password. After logging in, your requests will be listed and can be selected to review details.

Who do I contact with questions?

If you have questions contact the Office of Information Technology Support Desk.

Review process

How can I find out the status of a review?

There are three ways to find out the status of a review:

1. The Requestor, Procurement & Contract Services, or a member of the Office of Information Technology Support Desk staff can log in to Team Dynamix and look up the status.
2. The Requestor can review previously received ticket email messages.
3. Contact the Office of Information Technology Support Desk.

I am planning an IT project. Can I get an early review?

Yes; Enterprise Support, Information Security, and Accessible Technology team members are available to assist during the project planning phase. Assistance is available to ensure Requests for Proposals (RFPs) include necessary technology, operational, and integration requirements, information security and privacy requirements, accessibility requirements, and associated contract terms.

If you have questions contact the Office of Information Technology Support Desk and Procurement & Contract Services

Why can't I use Dropbox, iCloud, Google Drive, and SurveyMonkey?

In response to a CSU audit, a Cloud Computing Practice Directive went into effect to define campus cloud service standards as well as procedures on how to request an exception to acquire a non-standard cloud service. Office of Information Technology support is available to help and assist migrating to campus standard solutions.

Documentation

How can I add supporting documentation?

Navigate to your TAR Request in Team Dynamix and upload any attachments.

What is a VPAT?

A VPAT, or Voluntary Product Accessibility Template, is a self-assessment document completed by a vendor that provides relevant information on how their product or service claims to conform to Accessibility Standards.

What vendor documents are needed for cloud computing acquisitions that store data?

The vendor will be asked to provide one of the following cloud security assessment documents:

- A current SSAE-16 SOC 2 Type II (or equivalent third-party audited security standard).
- A current Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CSA CAIQ).
- An industry recognized current security certification or accreditation (e.g., FedRAMP authorized, ISO270xx, etc.).
- The Higher Education Cloud Vendor Assessment Tool (HECVAT).

What are the criteria for deciding which form can be used for a Cloud security assessment?

Based upon the type of data being stored in the cloud solution, only one of the following documents identified in the table below is necessary to meet the requirement.

DATA CLASSIFICATION TYPE OF DOCUMENTATION ACCEPTED

	Soc2 Type2	ISO 270xx Certification	FEDRAMP Authorized	HECVAT Full	Other CSA CAIQ, or TAR questionnaire
	x	x	x	x	x
– high record count	x	x	x	x	x
– small record	x	x	x		x
	x	x	x		x

For more information see: ICSUAM 8065.S003 Information Security Asset Management – Cloud Storage & Services

What is the risk acceptance process?

The risk acceptance process is used to document non-compliance with CSU policy. The process will involve a discussion between the Vice President of the requesting department, the campus Information Security Officer, and the Chief Information Officer. The process will be documented in writing and will list any mitigating controls that are used to reduce the risk, and indicates when the risk will be remediated or next reviewed. Once the process and mitigations have been documented, the Vice President capable of assuming the risk and the

Chief Information Officer must approve the risk acceptance. The risk acceptance documentation must be loaded into Team Dynamix for audit purposes.

Contracts

What are supplemental IT contract terms?

Supplemental IT contractual terms are CSU boilerplate contractual language that is edited as applicable to the technology deployment scope. The Information Security team determines if the acquisition requires a contract to protect the CSU liability. The applicable terms should be forwarded to Procurement & Contract Services to determine the best way to proceed.

How do I proceed if supplemental IT contractual terms are required?

If you have already submitted a requisition, forward the Master ticket to Procurement & Contract Services. If you were planning to use a P-card, contact Procurement & Contract Services to determine the best way to proceed.

How are contracts prepared and negotiated?

Contact Procurement & Contract Services for assistance preparing and negotiating contracts.

What if the vendor does not agree with Stanislaus State contractual terms?

The vendor can edit the draft contract with tracking enabled and identify the areas of disagreement or concern. The edited draft contract should be returned to Procurement & Contract Services, who coordinates vendor contract negotiations.