	Procedures for the Acquisition of Software	
	Responsible Administrative Unit: Information & Technology Solutions	**Procedure Contact:** Chief Information Officer, Monique Sendze msendze@mines.edu

1.0 PROCEDURE PURPOSE

The Colorado School of Mines ("Mines") is committed to ensuring that all software that is acquired and used at Mines furthers the teaching, learning, research, and business operations mission of Mines and meets Mines' security, accessibility, and privacy standards. As part of this commitment, Mines has established the following Procedures to:

- Ensure a software acquisition is necessary based on business needs.
- Evaluate and recommend the best software options.
- Certify that the selected software meets technical, privacy, security, accessibility and business standards.
- Make certain the software acquisition process is open to all those who have a need to know and participate.
- Ensure all software acquisitions are approved by the appropriate administrative departments.
- Confirm that training and support requirements are understood.
- Ensure that the total cost of ownership of the software is understood.

2.0 PROCEDURES

All software acquisitions must follow these Procedures. A **Software Acquisition Request form** must be completed to begin the review process. Software will not be installed without approval or without going through the review process. This process also applies to free/donated or low cost software and software to be used on a trial or pilot basis.

ITS plays a key role in supporting academic and administrative software and services and are available as early as possible to assist in this process by:

- Identifying software options to meet business needs
- Consulting for each of the steps described below
- Assisting with implementation requirements
- Facilitating the infrastructure to support the software
- Integrating the software with existing systems

- Providing troubleshooting services when applicable

2.1 Software and vendor services review.

- ITS must be included in all software acquisitions prior to obtaining the software to ensure compatibility with the campus infrastructure.
- ITS will ensure that the software meets operational and technical requirements including server configurations, operating systems, networking, and auxiliary or third-party software products (browser compliance, Java version, etc.) as well as the user needs.
- In addition to the software, ITS will also review data hosting and/or storage services, whether data is hosted internally or by the vendor (or a cloud agent acting on behalf of the vendor).
- ITS will assess the level of internal support necessary for continuous operation, and the support services that are either provided by or will need to be purchased from the vendor.
- ITS will look for those requests that should be handled as a project for implementation of the software requested. If necessary, a project request will be created.

2.2 Vendor software requirements.

- The software under review must provide a high quality service that improves our technology environment without jeopardizing network or server performance, data integrity or data security.
- All software that requires data exchange that may include protected information must comply with all applicable privacy laws, including those of the EU General Data Protection Regulation and other jurisdiction-specific law, as may be applicable.
- Vendors must provide evidence to illustrate the vendor has committed an appropriate level of resources to accessibility, data protection, and security. Vendors will be required to provide:
  - Completed HECVAT report for cloud-based services.
  - VPAT report as needed that illustrates the level of compliance with accessibility requirements.
  - SOC 1 or SOC 2 reports, their SSAE-16 or comparable compliance documents, PCI certification and/or self-assessment, and audit reports, as needed.
  - Documentation of retention and destruction procedures of confidential data.

2.3 Software demonstrations.

- ITS must be included with all stakeholders in vendor software demonstrations. ITS recommends comprehensive demonstrations prior

to the purchase of any software, and will work with vendors to arrange remote (video conference) demonstrations as needed.

- In cases where institutional data may be required for demonstration purposes, vendors must provide in advance all security compliance documentation as specified above, including written assurance that all data will be permanently removed from their systems following the demonstration.
- All privacy requirements apply to software demonstrations. Please refer to the Mines Data Policies.

2.4 Modifications to current licensing terms. Terms that are different or change the original acquisition terms shall be reviewed through the software acquisition approval process as if acquiring new software to ensure adherence to data security, privacy, operational integrity, and long-term sustainability standards.

2.5 Duplicate Software. It is the responsibility of the requestor to consult the list of software available at the software inventory website and or with ITS prior to submitting the software acquisition request to ensure that there are no other software currently licensed at Mines that could fulfill the needs for which the request is being made.

ITS reviewers in the process are responsible to be the second-level check on duplicate software with respect to risk, cost, labor, and functionality assessments. Identification of such assessments should be documented in the Team Dynamics (TDX) ticket.

Authority for rejecting a duplicate software purchase lies with the CIO or Director of Procurement. Prior to rejecting a duplicate software purchase, the CIO and or the Director of Procurement shall be advised by ITS reviewers of the duplicative software, the functionality of the duplicative software, the cost and the business risk of the duplicative software.

2.6 Renewals. Renewal of software is not automatic. All renewals will follow this procedure:

- Ask the software vendor if anything significant has changed with their answers to our questions since the approval process.
- If No, then Procurement will follow internal procedures to renew the software.
- If yes, then send back to ITS for the software approval process.

2.7 Pilots and Trials. New software acquired through a pilot or through a free trial becomes an integral part of the Mines IT systems. It is critical that this software is acquired in a manner that allows it to be evaluated for security and privacy risks and vulnerabilities.

2.8 **Under $5K Software.** All software under $5K will be subject to the same acquisition process regardless of payment type (e.g., OneCards) to ensure they meet Mines privacy, accessibility, and security requirements.

2.9 **Periodic review.** All software will be subject to periodic review for security, privacy, performance, behavior, financial, and contractual implications.

2.10 **Exceptions & Disciplinary Actions.** Requestors who have not followed this process will be asked to submit their request through this process. Failure to follow the process could result in delayed implementation, inability to implement the software, inefficient use of school funds, or disciplinary actions.

2.11 **System of Record.** TDX will be the system of record for Requests, Reviews and Approvals. Mines Contract and Research System will be the system of record for contracts.

2.12 **Internally Developed Software.** Software developed by Mines employees must protect data at the level required by the standard defined by the guidelines for how software is developed to ensure data privacy and system security and privacy.

2.13 **Review Completion.** Sign-off within the system indicates the request has been reviewed for the risks and requirements documented within the TDX task descriptions by area. It indicates necessary information has been reviewed to provide a recommendation to the business unit of the unmitigated risks to make an informed decision.

Sign-off will occur internally once area tasks are completed.

- Security – The Chief Information Security Officer reviews the requested software and making recommendations regarding the management of cybersecurity risks posed by the requested software.
- Licensing – ITS reviews the licensing technology to see if it appears to be one that will coexist in our current technological environment, or, if we can determine additional technology will be required up front (I.e. this license clearly will require a new license server or additional physical USB ports). This review is not exhaustive and may not catch requirements that may be discovered later on.
- Infrastructure – The Director of Infrastructure Solutions reviews the requested software and verifies that its introduction to the Mines IT infrastructure is sustainable and supportable; including making recommendations regarding compatibility.
- Privacy - The Privacy Compliance Director reviews the data sent/disclosed, received, collected, used, accessed, etc. within the

technology under review and makes recommendations to manage the privacy risks with the vendor.

- Research – The Director of Cyberinfrastructure and Advanced Research Computing reviews software used for research, both on local and shared infrastructure.
- Online/VDI – The Online Program Manager and Director of User Experience and Support Services reviews and approves software used in online courses and VDI environment to ensure there is appropriate support for implementation and planning for future growth.
- Lab –The Director of User Experience and Support Services reviews and approves software used in the teaching classrooms and labs. This review is to ensure the software will run on the current operating systems supported in the classrooms and labs.
- Data Stewards – Review and approve the data identified to be transmitted to the vendor.
- Export Controls – The Research Compliance Officer reviews and makes recommendations to manage the export control risks.
- Project Management – The Project/Portfolio Manager reviews requests and identifies those that should be handled as a project.
- Accessibility – The CIO or their designated representative will make decisions regarding accessibility based on recommendations that come out of the accessibility committee. The CIO or their designated representative will make decisions regarding accessibility based on recommendations that come from the accessibility technologist as a member of the accessibility committee. The accessibility technologist reviews software for compliance with accessibility laws and regulations in consultation with the accessibility committee when appropriate or necessary.

Each person is responsible for checking in the system for ticket updates. Notifying “ITS Leadership” will not be standard practice.

2.14 Software Inventory List. The software inventory list will be maintained by ITS. On an annual basis, ITS and the Controller’s Office will review and update the software inventory list.

2.15 Types of Software. Software is a general term primarily used for digitally stored data such as computer programs and other kinds of information read and written by computers. Computer software can be put into categories based on common function, type, or field of use. Below are some broad classifications:

- ***Application software*** is the general designation of computer programs for performing tasks. Application software may be general purpose (word processing, web browsers, etc.) or have a specific

purpose (accounting, truck scheduling, etc.). Application software contrasts with system software.

- ***System software*** is a generic term referring to the computer programs used to start and run computer systems including diverse application software and networks.
- ***Computer programming tools***, such as compilers and linker, are used to translate and combine computer program source code and libraries into binary executables.
- ****as-a-service*** is a way to describe how you can use the cloud for delivery of software and IT infrastructure. Software-as-a-Service (SaaS) uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a web browser without any downloads or installations required, although some require plugins. Examples of SaaS include: Google Apps, Office365, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx, Zoom, Dropbox, Mailchimp, SurveyMonkey, Qualtrics, DocuSign, Slack, etc. Cloud platform services, or Platform as a Service (PaaS), are used for applications, and other development, while providing cloud components to software. Examples of PaaS include: Apprenda, AWS Elastic Beanstalk, Heroku, Windows Azure, Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud, etc. Cloud infrastructure services, known as Infrastructure as a Service (IaaS), are self-service models for accessing, monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, networking, and networking services (e.g. firewalls). Instead of having to purchase hardware outright, users can purchase IaaS based on consumption, similar to electricity or other utility billing. Examples of IaaS include: Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE), Rackspace, etc.

- **Trial vs. Pilot use of Software:** Pilots and trials are a good way to reduce risk on a software implementation to make sure it fits well into the implementing organization's technical and non-technical systems and processes and that it fulfills the functional needs for which it is being considered.

    - **Pilot**: The purpose of the pilot is primarily to prove viability, not deliver an agreed outcome. There is a clear need for a control structure that enables prompt cancellation but also allows for the potential for radical changes in scope and direction if required. The intention is to create a controllable budget for people and supplies that will enable the project team to confirm that the underlying idea is sound. The pilot will confirm viability and scalability and enable proposed processes and procedures to be tested. It will confirm the

appropriateness and safety of the software proposed and also confirms that any working practices are safe and comply with organizational/statutory standards. It also enables the benefits to be tested and a more reliable investment appraisal to be created for the main project. It can be a stage gate for software implementation to scale from and take the pilot to production.

- **Trial**: A trial is a small-scale implementation planned before the main rollout of the software. It enables the project team to test the software and the effectiveness against the functional and technical requirements. There is a clear need for a control structure that enables prompt cancellation but also allows for the potential for changes in approach, scope and direction if required. The trial enables a more accurate budget and plan to be produced for the main roll out and as with the pilot stage offers an opportunity for the benefits to be revisited in the light of practical rollout experience. A trial does have some down sides, care needs to be taken to ensure that scalability is proven during the process and prolonged run.

3.0 HISTORY AND REVIEW CYCLE

The procedures within this document will be reviewed at least annually, or as needed by the Responsible Administrative Unit.

Issued: February, 27, 2020.