



DATA SECURITY IN PROCUREMENT CONTRACTS

Supplier contracts/agreements that include any of the following components must be reviewed by Purchasing Services, Caltech's Chief Information Security Officer, and the Office of General Counsel:

- Hosted software services in which members of the Caltech community log into
- Caltech will send data (other than public data) to the supplier
- On-site data processing software

Expect the data security review to add an additional 7-10 days in processing time.

PURCHASING SERVICES

As part of the review process, please be prepared to answer the following questions from Purchasing Services:

- Has Caltech done business with the supplier in the past?
- Is the supplier a reputable company with higher education experience?
- Is there a contract for review? Does it include data security provisions?

INFORMATION SECURITY OFFICE

As part of the review process, please be prepared to answer the following questions from the Information Security Office:

- What data will be shared with or stored by the system? Is it considered non-public?
- What areas of the Caltech community will be using this system?
- Does the supplier have an independent audit opinion about the security controls of their system?
- Will the supplier provide us with a HECVAT documenting their information security program (Higher Education Community Vendor Assessment Tool - see <https://www.ren-isac.net/public-resources/hecvat.html>)?
- Has the supplier suffered a data breach in the last five years?
- Additionally, please collect system documentation that is pertinent to the security of the system to provide to the security team. The team will most likely request a

meeting with the supplier to answer follow-on questions and develop a full understanding.

OFFICE OF GENERAL COUNSEL

As part of the review process, please be prepared to answer the following question(s) from the Office of General Counsel:

- What is the name and contact information of the company's point person for this agreement?