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
- 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, as outlined below, and/or a Data Protection Agreement/Addendum (DPA)?

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?
- ☐ Collect documentation that is pertinent to the security of the system to provide to the security team. The team may request a meeting with the supplier to answer follow-on questions (as outlined below) in order to develop a full understanding.

Additional security information required for the contract:

☐ Data Encryption Requirements:
- What encryption standards must be used for data at rest and in transit?
- Ensure the contract specifies the use of strong encryption methods (e.g., AES-256 and TLS 1.2+).

☐ Access Control Policies:
- What access control mechanisms are required to protect sensitive data?
- Include clauses that mandate multi-factor authentication (MFA) and role-based access controls (RBAC).

☐ Incident Response and Notification:
- What is the supplier's incident response plan, and how quickly must they notify you of a data breach?
- Specify the timeframe for breach notification (e.g., within 24 hours of discovery).

☐ Regular Security Audits:
- How often will the supplier undergo security audits, and will they provide audit reports?
- Include a clause requiring annual security audits and the provision of audit reports to your department.

☐ Data Retention and Deletion:
- What are the supplier's data retention and secure deletion policies?
- Ensure the contract includes clear terms for data retention periods and secure deletion methods.

☐ Compliance with Security Standards:
- What security standards and certifications must the supplier comply with (e.g., ISO 27001, SOC 2)?
- Include a clause requiring compliance with relevant security standards and certifications.

☐ Employee Security Training:
- What security training programs are provided to the supplier's employees?
- Mandate regular security training and awareness programs for all employees handling your data.

☐ Physical Security Measures:
- What physical security measures are in place to protect data centers and other facilities?
- Specify requirements for physical security controls, such as access controls and surveillance.

☐ Business Continuity and Disaster Recovery:
- What are the supplier's business continuity and disaster recovery plans?
- Include clauses requiring robust business continuity and disaster recovery plans.

☐ Data Integrity and Quality:

- How does the supplier ensure the integrity and quality of the data they process?
- Mandate regular data integrity checks and quality assurance processes.

☐ Third-Party Risk Management:
- How does the supplier manage risks associated with their subcontractors and third-party vendors?
- Require the supplier to ensure that their subcontractors and third parties comply with the same security standards.

☐ Security Governance and Policies:
- What governance structures and policies does the supplier have in place to oversee their security program?
- Include clauses that require the supplier to maintain comprehensive security policies and governance frameworks.

☐ Right to Audit:
- Does your organization have the right to audit the supplier's security practices?
- Include a right-to-audit clause that allows Caltech to conduct security audits of the supplier.

☐ Data Ownership and Control:
- How is data ownership and control defined in the contract?
- Clearly define data ownership and ensure Caltech retains control over its data.

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 contract/agreement?