Grayson College
Third-Party Information Security Standard

History

Version No.	Issue Date	Status	Reason for Change
v1.0	10/15/2020	Draft	

Review

Reviewer's Details	Version No.	Date

1. POLICY

As cybersecurity attacks become increasingly common and sophisticated and with the associated risks of outages, data loss or brand damage, the Grayson College must find ways to effectively manage these risks including in its agreements with vendors or requests for proposals (RFPs). An agreement or RFP does not replace diligence; however, given the frequency of security breaches today, effective language within such documents is used to ensure Vendor compliance with the College's Information Security Policies is a critical first line of defense.

2. SCOPE

The objective of this standard is to establish requirements for engaging third-party service providers that access, process, store, communicate or manage Grayson College systems, information, or information processing facilities. These documents are for business use and can be released to vendors, business partners, individuals, or organizations that have a signed Non-Disclosure Agreement on file; in addition, they must have a valid business purpose for receiving the information

3. POLICY STATEMENT

4.

Agreements and RFPs between the College and Vendors must have built-in protections against specific risks. Best practices dictate leading with a College-defined agreement and then scrutinizing the Vendor's suggested changes especially when changes create unacceptable risks to the College. Where this is not feasible, this guide helps College personnel to identify and propose key terms and conditions for insertion into the Vendor's agreement. The information security sections are key, but implications are also present for the definitions and standard contract sections. This type of comprehensive review is necessary to ensure adequate protection to Grayson College Data.

The Information Security Officer ("ISO") must analyze the risks, using the Grayson College Risk Assessment Guidelines document, not transferred by the contract and determine trade-offs. If risk mitigation is unavailable contractually, the ISO must work with the Grayson College leadership to understand what trade-offs are available through analysis of technology and business solutions. For this reason, Grayson College must have a clear understanding of the Vendor's information security and privacy commitments as well as what commitments the Vendor is declining to make. It is essential to emphasize the importance of visibility into the security posture of cloud-based vendors when there is less flexibility to dictate the specific controls that are adopted.

This document provides guidance to Grayson College on a comprehensive recommended framework for achieving compliance with information security requirements in agreements and RFPs. Grayson College should use this document to ensure that each requirement is met for a given area or system. An area could be as broad as an entire department or as narrow as a single research project. Similarly, systems may range from enterprise systems to something extremely narrow such as document storage for a single user. Appendix A is a checklist to ensure each section and subsection is addressed when reviewing an agreement or RFP. Appendix B contains sample language that may be adopted.

Information security terms and conditions in agreements and RFPs may be satisfied in a manner other than the recommended framework detailed in this document. The Grayson College Information Security Officer (ISO) is committed to providing solutions that enable Policy compliance and make compliance reporting easy. However, business requirements may necessitate the implementation of alternate solutions to satisfy Policy compliance and/or manual compliance reporting. For additional guidance, please contact the Information Security Officer.

5. REQUIREMENTS

A. THIRD-PARTY ASSESSMENT

A review of potential third-party service providers should be conducted prior to any RFP, agreement, or contract award and actual information access or transfer. The use of this document and the Grayson College Vendor Security Questionnaire should be used. This review will include a determination of the third-party's security policies, procedures, and capabilities as they relate to the services being provided. Identified shortcomings should be remediated before a contract is signed, and access is granted.

B. THIRD-PARTY AGREEEMENT TERMS

All third-party service provider agreements that involve the accessing, processing, storing, communicating, or managing of Grayson College information or information processing facilities must address all of the following areas:

1. Security requirements in compliance with Grayson College information security policies and standards; provide a recent, completed within the last six months, external security audit SOC Report findings
2. Compliance with any relevant local or global data privacy legislation
3. Third-party expectations related to information security incident response specific to any Grayson College information
4. Provision for Grayson College to perform on-site auditing to verify compliance with the agreement terms

Non-disclosure agreements are to be used when the information being disclosed to the third-party is confidential.

C. INFORMATION TRANSFER

All third-party service provider agreements should include a provision to notify Grayson College before the access or transfer of College information to a sub-contractor. Grayson College should perform a risk assessment of the sub-contractor using the Grayson College Vendor Security Questionnaire and include a right to audit clause.

A Data Transfer Process should define what information can be released to whom and how it should be transferred. This process must be followed for each release of electronic information to the third-party.

The transfer of confidential information must be done using secure current Grayson College approved mechanisms.

The agreements should include specific terms for the disposal or return of College information upon fulfillment of the business purpose.

D. ONGOING SECURITY MONITORING

The service provider's security environment must be reviewed bi-annually to determine the adequacy and compliance in accordance with the agreement. The review will include obtaining a SOC report, performing an on-site audit, etc.

When there are revisions to a third-party service agreement, there must be a review by the Information Security Officer of any potential security risk implications.

6. TRAINING

These Third-Party Information Sharing Security Standards shall be provided to each of Grayson College 's employees who manages systems, or the processes of Data owned or controlled for Grayson College. Each such individual is also required to complete a training program on information security and these standards. The Information Security Officer shall be responsible for introducing the security relating information to new employees as part of Grayson College onboarding process, annually, and when changes to the program are made.

7. DISCIPLINE FOR VIOLATION OF THE PROGRAM

Consistent with Grayson College policies, the Information Security Officer is authorized by the Grayson College President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the college community.

Administrators must ensure that measures are taken within their department to comply with this program and its related standards, guidelines and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the Information Security Officer. Approved requests will be reviewed annually to determine if an exception is still warranted.

Grayson College reserves the right to temporarily or permanently suspend, block, or restrict access to college information technology resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of Grayson College information technology resources;

to protect Grayson College from liability; or to enforce this policy and its related standards and practices.

Failure to adhere to the provisions of this policy statement or the appropriate use policy statement may result in:

- ·Suspension or loss of access to Grayson College information technology resources
- ·Appropriate disciplinary action under existing procedures applicable to students, faculty and staff, and
- ·Civil or criminal prosecution

Potential violations will be investigated in a manner consistent with applicable laws and regulations, and Grayson College policies, standards, guidelines and practices (TAC§202.72) (TAC§202.73).

The Vice President for Administrative Services or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate college officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Third-party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to Grayson College.

Appeals of college actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for Grayson College students and employees.

14. POLICIES CROSS-REFERENCED

The following Grayson College policies provide advice and guidance that relates to this Program:

A. Grayson College Written Information Security Program
B. Grayson College Vendor Security Questionnaire
C. Grayson College Risk Assessment Guidelines

.

APPENDIX A

Checklist for Information Security in Agreements: Transfer of College Data to Third-Party Systems

1. Definitions
   1.1. Authorized Users
   1.2. Confidential Information
   1.3. College Data
   1.4. Data Compromise
   1.5. Information Security Incident
2. Concepts
   2.1. College Data Protection
   2.2. Access Control
   2.3. Patch Management
   2.4. Scanning and Penetration Testing
   2.5. Encryption
   2.6. Security Development
   2.7. Deterioration and Degradation
3. Notification
   3.1. Notification of Data Compromise
   3.2. Incident Reporting
   3.3. Third-Party Requests
4. Workforce Security and Geographic Location
   4.1. Background Checks
   4.2. Location
5. Audit
   5.1. Security Reviews
   5.2. Reports
   5.3. Additional Audits at College Request
6. Destruction and Return of College Data

APPENDIX B

Information Security Terms and Conditions in Agreements

1. Definitions

1.1 Authorized Users *Explanation*: To mitigate risks, define who has access to College Data and how they will obtain permission. Limiting the definition of "Authorized Users" will ensure access is not inappropriately authorized and trigger vendor processes for approval of any additional users who need access to College Data that leverage the definition in the Information Security section of the agreement.

Sample Language: "Authorized User" means and is limited to (1) Authorized Employees; and (2) Vendor's subcontractors, agents, and auditors who have a need-to-know or otherwise access data to enable the Vendor to comply with the Agreement, and who are bound in writing by confidentiality obligations sufficient to protect College Data in accordance with the terms hereof.

1.2 Confidential Information *Explanation*: Clearly define what is considered confidential both legally and in terms of privacy, so that the proper protections are in place for the information. Confidential Information should include not only proprietary information (intellectual property, trade secrets and patents) but also sensitive commercial or research information, financial information, and private information of employees, students, and other individuals (addresses, phone numbers and account information). The agreement should use this defined term to set parameters around the conditions of data usage, disclosure permission and treatment of the data if either party is legally compelled to disclose the information. Use of Confidential Information should be limited to fulfilling the terms of the contract only. If legal disclosure is required, the parties must notify each other and protect against further disclosure.

Sample Language: "Confidential Information" means any non-public information that is confidential or proprietary to a party and is disclosed or becomes known pursuant to this agreement. Except to the extent information is required to be kept private or confidential pursuant to other law, regulation, or policy, "Confidential Information" does not include information that is or becomes generally available or known to the public through no act of omission of the receiving party; was received lawfully from a third-party through no breach of any obligations of confidentiality owed to the disclosing party; or created by a party independently of its access to or use of other party's information.

1.3 College Data *Explanation*: A subset of Confidential Information, agreements or RFPs should clarify ownership of College Data and protect the data that the College generates, updates, receives, and processes in the course of using the Vendor's services. Having a broad definition of College Data ensures that there is no doubt about data that is protected and under what circumstances the Vendor can access the data.

Sample Language: "College Data" means any and all data, information, text, graphics, images, works and other materials that are collected, loaded, stored, accessible,

transferred through and/or accessed by the College in the course of using the Vendor's services, including, but not limited to: (1) updates, modifications and/or deletions; (2) all of the results from the use of services; and (3) all information and materials that are developed or acquired prior to, or independently of, the Agreement. College Data is Confidential Information.

1.4 Data Compromise *Explanation*: Define data compromise as actual or reasonably suspected unauthorized access of datasets and include the parameters upon which the Vendor needs to protect against and provide notice of any data compromises.

Sample Language: "Data Compromise" means any actual or reasonably suspected unauthorized access to, or acquisition of, data that compromises the security, confidentiality or integrity of the data or the ability of the College to access the data.

1.5 Information Security Incident *Explanation*: The agreement or RFP should include the requirements and responsibilities in reporting and responding to Information Security Incidents to minimize negative impacts to the confidentiality, integrity, and availability of College Information Resources and College Information. A comprehensive definition of "Information Security Incident" will ensure proper coverage. This definition is constructed to enable overlap between the concepts of incident reporting and audit reports. By including imminent threat in this definition, the College will require the Vendor to report significant vulnerabilities under the Incident Reporting clause. That clause also explicitly calls for reporting of the findings of vulnerability scans. Ultimately, the goal is to ensure sufficient visibility for the College into the security of College Data held by the Vendor.

NOTE: In order to ensure compliance with Texas law, do not permit deletion of "reasonably suspected." It is recommended that the Vendor may be permitted to remove either the phrase 'imminent threat' from this definition or the Reports clause from the Notifications section, but not both.

Sample Language: "Information Security Incident" means any actual or reasonably suspected incident, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of College Data; interference with information technology operations; or significant violation of the College's information security policy or the information security provisions of this Agreement.

All systems containing College Data must be designed, managed, and operated in accordance with information security best practices and in compliance with all applicable federal and state laws, regulations and College Information Security policies. To diminish information security threats, the Vendor must (either directly or through its third-party Vendors) meet the following requirements, where applicable.

2.Concepts

2.1 College Data Protection *Explanation*: Negotiate the following security protection articles to ensure security and mitigate risk. If unsure about the implications of any proposed deviation, confer with the Information Security Officer. Cross-reference the Definitions section, any applicable regulations and exhibits to make this section even stronger.

Sample Language: All facilities used by or on behalf of the Vendor to store and process College Data will implement and maintain administrative, physical, technical, and procedural safeguards in accordance with industry best practices at a level sufficient to secure such data from unauthorized access, destruction, use, modification or disclosure. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event, less than reasonable in view of the type and nature of the data involved. The Vendor must maintain the administrative, physical, technical and procedural infrastructure associated with the provision of services to the College in a manner that is, at all times during the term of this Agreement, at a level equal to or more stringent than those specified by the parties to this Agreement.

2.2 Access Control *Explanation:* To mitigate risks, defining who has access to your data and how they will obtain permission is crucial. Limit access by ensuring your definition of "Authorized User" is appropriately narrow and create processes for access approval that leverage your definitions.
Access Control is the selective restriction of access to a resource. Three critical aspects of documenting access control are:

Establishing appropriate policies and procedures exist that define the rules and methods for making access decisions; Ensuring the Vendor will review access decisions (authorizations) for compliance with such policies and procedures; and Allowing for College review of actual access against authorizations – to confirm the implementation of access matches the authorizations.

Sample Language: The Vendor will control access to the College's Data, limiting access to Authorized Users who have a legitimate need-to-know based on individual work assignment for the Vendor. The Vendor will trace approved access to ensure proper usage and accountability, and the Vendor will make such information available to the College for review, upon the College's request and not later than five (5) business days after the request is made in writing.

2.3 Patch Management *Explanation*: When Vendors discover an error in their software, they usually release a piece of free software - called a patch, hotfix, or service pack - to correct it. But many IT professionals fail to properly install patches to fix their organization's software vulnerabilities. Some Vendors resist spending the time to patch all software or even find out what patches exist. Or, they do not want to install a patch because they are worried it will cause problems with another program. But it is essential to get the Vendor to properly install appropriate software patches, whether on their systems or on College equipment being serviced by the Vendor.

Although most software errors, or bugs, are harmless, some can leave your computer systems and the data they contain vulnerable. A good way to keep this from happening to the College is to require Vendors to create a patch management policy spelling out how to find, test, and install software patches or to receive assurance from the Vendor of their commitment to complying with the College patch management policy.

Sample Language: Vendor will carry out updates and patch management for all systems and devices in a timely manner, applying security patches within five (5) business days or less based on reported criticality. Updates and patch management must be deployed using an auditable process that can be reviewed by the College upon the College's request and not later than five (5) business days after the request is made in writing. An initial report of patch status must be provided to the College prior to the effective date of this Agreement.

2.4 Scanning and Penetration Testing *Explanation*: A vulnerability scan or penetration test seeks to identify weaknesses in hardware, software, and the overall network. Vendors that handle sensitive College Data must guard against intrusion into their systems by conducting regular network and application vulnerability scanning and penetration testing through a qualified and credible resource. Scans should be performed on a frequent and regular cadence with penetration testing being done once annually at a minimum, for Vendors who store College Data.

Sample Language: Prior to the Effective Date of this Agreement, and at regular intervals of no less than annually and whenever a change is made which may impact the confidentiality, integrity, or availability of College Data, and in accordance with industry standards and best practices, Vendor will, at its expense, perform scans for unauthorized applications, services, code and system vulnerabilities on the networks and systems used to perform services related to this Agreement. An initial report must be provided to the College prior to the Effective Date of this Agreement. Vendor will provide the College the reports or other documentation resulting from the audits, certifications, scans and tests within five (5) business days of Vendor's generation or receipt of such results. The Vendor will, if such results so require, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement and provide the College with written evidence of remediation. The following audits, certifications, scans, and tests are required:

> *A vulnerability scan performed by a qualified and credible third-party of the Vendor's systems and facilities that are used in any way to deliver services under this Agreement;*
> *A formal penetration test performed by qualified personnel of the Vendor's systems and facilities in use in any way to deliver services under this Agreement; and*
> *The College may require the Vendor to perform additional audits and tests, the results of which will be provided to College within seven (7) business days of Vendor's receipt of such results.*

2.5 Encryption *Explanation*: Many information security and privacy regulations require data protections such as encryption. While not a guarantee, encryption is an easy way to give added assurance that the confidentiality of data is protected. However, there will sometimes be circumstances where encryption poses a challenge. High performance computing, for example, would suffer from performance degradation if disks were encrypted. Where appropriate, the Vendor should agree to encrypt College Data in their possession. When that cannot be achieved, insist upon reviewing a SOC2 or other third-party report describing the mitigating controls that are in place; the Information Security Officer can assist with this review.

Sample Language: All systems and devices that store, process and/or transmit Confidential Information must use an industry standard encryption protocol for data in transit and at rest.

2.6 Security Development *Explanation*: When buying third-party software or outsource application development, you subject your data (and potentially other College Information Resources) to the vulnerabilities that the Vendor fails to eradicate. Vendors that have implemented a secure Software Development Life Cycle (SDLC) enhance the security of applications developed by them. The failure to use SDLC is an unacceptable weakness in the security posture of the College, as these products, which are acquired from third-party vendors, are subject to security vulnerabilities. Thus, the Agreement should require vendors who develop software for the College to use an SDLC.

The language below establishes the minimum requirements for secure software development performed by Vendors on behalf of the College and ensures the authority of the College to validate. Authority to review the actual findings of scans is covered in section 5.2 for Reports.

Sample Language: Vendor will use secure development and coding standards; including secure change management procedures in accordance with industry standards. The Vendor's web applications must meet OWASP Application Security Verification Standards (ASVS). The Vendor will perform penetration testing and/or scanning prior to releasing new software versions. Vendor will provide internal standards and procedures to the College for review upon the College's request.

2.7 Deterioration and Degradation *Explanation*: Vendors must have a system for controlling and monitoring proper handling, preservation, storage, and transmission processes to protect the quality of College Data and systems and to prevent their damage, deterioration and degradation. This is particularly critical when the Vendor is in possession of unique copies of any College Data or otherwise is responsible for preservation of systems or data critical to the business of the College.

Sample Language: Vendor will protect College Data against deterioration or degradation of quality and authenticity, including, but not limited to, annual data integrity audits performed by an independent, external organization.

3.Notification

3.1 Notification *Explanation*: It is critical that the College maintain good communication with Vendors on matters of information security. Clearly spell out the obligation of the Vendor to maintain these communications and include the details of how and when to communicate. The ISRM in the unit responsible for the agreement should also be looped in to be sure that the reports are tracked, monitored and responded to.

Sample Language: Any notices or communications required or permitted to be given to the College under this Agreement must be (1) given in writing and (2) transmitted by electronic mail transmission (including PDF), to the College Information Security Officer at security@grayson.edu. Any such notice or communication must be deemed to have been given on the day such notice or communication is sent electronically, provided that the sender has received a read receipt or other replied acknowledgement of such electronic transmission.

3.2 Notification of Data Compromise *Explanation*: If, and when, a data breach occurs or is suspected, it is necessary to require the Vendor to notify the College as soon as it is aware of the data breach so actions can be taken to protect College services, data, and personnel. Most Vendors will state that they will notify within 48 hours. The College Information Security Officer recommends having the Vendor notify as soon as they are reasonably aware or within 24 hours at the latest. Some Vendors will also provide remediation assistance when a data breach occurs. Ensure that data breach notification is consistent with any regulatory and other contractual obligations. Strive for remediation assistance where possible.

Sample Language: Unauthorized access or disclosure of nonpublic data is considered to be a breach. The Vendor will provide notification as soon as it is aware of the Data Compromise or breach to the College Information Security Officer at security@grayson.edu. When the Vendor is liable for the loss, the Vendor must bear all costs associated with the investigation, response and recovery from the breach, including, but not limited to, credit monitoring services with a term of at least three (3) years; mailing costs; website; and toll-free telephone call center services. Any limitation on liability in this Agreement or elsewhere is void to the extent that it relieves a Vendor from its own negligence or to the extent that it creates an obligation on the College to hold the Vendor harmless.

3.3 Incident Reporting *Explanation*: Information Security Incidents may not meet the threshold of being a breach, but may still impact the confidentiality, integrity, or availability of College Data. Further, the frequency and severity of incidents may offer insights into the likelihood of future breaches. Where possible, request that information security and privacy incidents be reported to the College.

Sample Language: Vendor will report all other Information Security Incidents to the College within 24 hours of discovery.

3.4 Third- Party Requests *Explanation*: Third parties will, under certain circumstances, request Vendors to provide access to data owned by their customers. In some situations, the Vendor may be legally obligated to fulfill the request. When these situations occur, the College can mitigate any risks of such disclosure if we are notified right away.

Sample Language: The Vendor will notify the College immediately if the Vendor receives any third-party request for College Data, including but not limited to a subpoena, a court order, a public records request, a request directly from a data subject, or other type of inquiry or demand; or the location or method of transmission of College Data is changed. All notifications to the College required in this Information Security paragraph will be sent to the College Information Security Officer at security@grayson.edu, in addition to any other notice addresses in this Agreement. In all such instances, to the extent legally feasible, the Vendor will not provide any College Data to such third-party and will instead direct the requestor to the College.

4.Workforce Security

4.1 Workforce Security and Geographic Location *Explanation*: Many universities today rely upon more than just their own employees and look to vendors, agencies, contractors and other non-employee workforce to get the job done. Screening programs for these non-employees are often regulatorily required and, in any case, are a critical best practice to protect information security. Vendors may have a screening process in place, but the background screening industry lacks standardization, so that alone is not reliable. Consider the nature of the College business the Vendor will support and choose constraints on when and how background checks will be performed. Consider whether it is appropriate to limit the locations where non-employees may work when fulfilling the Vendor's contractual obligations.

Sample Language: The Vendor will comply with workforce location and security clauses as outlined in this Agreement. Additionally, the Vendor will ensure their workforce is properly trained on information security and privacy practices of the College and on any information security or privacy regulations, as required by applicable rules. The Vendor must promote and maintain an awareness of the importance of securing the College Data to its employees and agents.

4.2 Offshore *Explanation*: With the cloud, data can be stored and supported anywhere in the world. Quite often, providers will ask to acknowledge that the data could be stored or serviced offshore. If control over where the data sits is required, this must be discussed with the Vendor and determine whether or not appropriate controls can be put in place to keep the data and support where required.

Where College Data under the Agreement may include the personal data (as defined in GDPR) of individuals in European Union, data should remain in the United States if possible.

Sample Language: The College may select or restrict where College Data will be stored and where College Data can be processed, and the Vendor will store and/or process it there in accordance with the service terms. If a data location selection is not covered by the service terms (or a Data Location Selection is not made by the College with respect to any College Data), the Vendor will not be restricted in the selection of College storage or processing facilities. Any services that are described in this Agreement that directly serve the College and may involve access to sensitive College Data or development or modification of software for the College will be performed within the borders of the United States. Unless stated otherwise in this Agreement, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of this Agreement. This provision applies to work performed by subcontractors at all tiers and to all College Data.

4.3 Background Checks *Explanation*: If the Vendor is performing a function requiring access to personal data or regulated data or where there are specific security or governance concerns, include a background check on the Vendor's employees as part of the contract and ask for verification of the Vendor's processes.

Sample Language: The Vendor must conduct background checks and not utilize any individual to fulfill the obligations of this Agreement, including subcontractors, if such individual has been convicted of any crime involving dishonesty or false statement including, but not limited to fraud and theft, or otherwise convicted of any offense for which incarceration for a minimum of one (1) year is an authorized penalty. Any such individual may not be an "Authorized User" under this Agreement.

5.Audit

5.1 Audit *Explanation*: Vendors generally will certify and validate the security standards they offer. They usually do not allow individual organizations to audit their environments. Allowing each organization to audit would be time-consuming and disruptive to the environment and would potentially impact any other client of the Vendor. If units have specific requirements, the unit will want to ensure the Vendor meets them, or at least, address them before contracting.

Sample Language: The Vendor will, at its expense, conduct or have conducted such audits and certifications as defined under this section at least annually, and immediately after any actual or reasonably suspected breach. The Vendor will provide the College the results of any such audits as defined under this section, along with the Vendor's plan for addressing or resolving any shortcomings identified by such audits, within seven (7) business days of the Vendor's receipt of such results.

5.2 Security Reviews *Explanation*: One way to better ensure the protection of College Data either when it is transferred to a third-party or when purchasing third-party software for use within the College environment is to ensure the Vendor performs a SOC 2, SOC for Cybersecurity, or similar audit of their security policies, procedures and

controls. (NOTE: SOC 1 reports are not useful in the context of security. SOC 1 reports are financial controls and can sometimes be confused with security policies.) SOC 2 reports may be Type I or Type II. Type II reports are preferred as they give insight into the function of the Vendor's organization over time; as opposed to the snapshot view afforded by Type I reports. The Information Security Officer can assist with this review. Contracts involving highly sensitive data may require more frequent review.

Sample Language: The Vendor will complete one of the following audits at least annually and immediately after any actual or reasonably suspected Data Compromise: SOC 2 Type I or II, SOC for Cybersecurity, or an accepted Higher Education Cloud Vendor Assessment Tool. Evidence must be provided to the College prior to the Effective Date of this Agreement and at least annually thereafter.

5.3 Reports *Explanation*: In cases where the Vendor does not participate in any acceptable third-party reviews, certifications, or validations, or is unwilling to share those findings with the College, residual information security risks can be mitigated by including provisions for the College to perform similar reviews of reports generated by the Vendor. These reports must provide the College with insights into Vendor practices that directly impact the security of College Data and those that have implications on the ability of the College to meet its own information security and privacy commitments.

Vendors may resist the requirements to share findings of vulnerability scans with customers. In these situations, be sure that the phrase 'imminent threat' is present in the definition of Information Security Incident and that the Incident Reporting clause remains substantially intact so that the requirement to report these vulnerabilities remains in place.

Sample Language: The College reserves the right to annual, at a minimum, review of: Vendor access reports related to access to College Data; Vendor patch management process, schedules, and logs; findings of vulnerability scans and/or penetration tests of Vendor systems; and Vendor development standards and processes.

5.4 Additional Audits at College Request *Explanation*: Especially where the visibility needs of the College are not being sufficiently satisfied by the commitments made for either periodic third-party review or other reports, it is often helpful to include a provision that allows the College the flexibility to make additional requests for information.

Sample Language: The College may require the Vendor to perform additional audits and tests, the results of which will be provided to the College within five (5) business days of the Vendor's receipt of such results.

6.Destruction and Return

Destruction and Return of College Data *Explanation*: At the end of the agreement, whether it is by termination or natural expiration, ensure that College Data is returned, all copies are destroyed, and a certification of its destruction is received. This protects against unintentional exposure of Confidential Information and infringement on

College intellectual property rights. Ask for assistance and sufficient time to move the data after termination, ensure that the Vendor notifies the College in writing when the data is ready to be moved, and then waits for authorization before deleting data.

Sample Language: Except as permitted in other areas of the Agreement, the Vendor will promptly return the College's Confidential Information upon termination of this Agreement, the final performances of services under this Agreement, or upon the request of the College, whichever comes first. In the event the Vendor has non-unique copies of the College's Confidential Information that are also held by or returned to the College, the Vendor may, in lieu of returning such non-unique copies, destroy such Confidential Information in all forms and types of media and provide written confirmation or certification of such destruction.