REGIS UNIVERSITY

Information Technology Services

Information Technology Vendor Vetting and Third-Party Electronic-Data Release Authorization Form

_____

Vendor

_____

Year established

_____

Product/Service (If Applicable)

_____

Year Product/Service introduced:

_____

Requester:

_____

Requesting Department:

Introduction and Instructions

Overview: The purpose of this document is to gather information and documentation necessary to evaluate potential new IT vendor relationships and whether university-owned data can be safely and securely entrusted to the third-party vendor.

Following is the process for requesting release of data to third parties:

1. A university representative (the person making the request for release or the person largely responsible for facilitating the release) completes Section 1 of the request.

2. The vendor to whom the data is being released completes Section 2 and provides all available and appropriate documentation to the university representative.

3. The completed release is returned to the university's Information Security Officer (ISO) for review and evaluation.

4. The ISO completes a written analysis of the request and forwards the release request to appropriate data owners (Vice Presidents) and reviewers (other university representatives with particular data oversight, e.g. University Risk Manager, Registrar, etc.) for approval. The exact list of approvers will depend on the nature of the data being requested for release.

5. The approvers will indicate their decision on the signature sheet and return the packet to the university's ISO.

6. The university's ISO will notify the university representative and ITS staff when the release is fully completed.

Scope:

The process described in this packet applies to any university-owned information in electronic format that meets any of the following conditions:

1. Information that is extracted from any electronic database on university systems, including enterprise systems, such as Datatel/Coleague, and any departmental or individual databases, and is to be transferred to a third-party vendor for any purpose and in any format.

2. Information that is to be stored/hosted on electronic data systems of third-party vendors but no extract of university-owned information from any university systems is required.

Term:

This release authorization will remain in effect until the termination of the agreement or until the status of the vendor's policies, procedures, or insurance coverage changes.

To Data Requesters (Regis University Representatives):

Please use the checklist on Page 3 to guide you through the process. You are responsible for completing Section 1 of the document and the vendor to which the university is releasing data is responsible for completing Section 2. You will then gather the completed materials together and submit them to the University's Information Security Officer for completion. The ISO will review and gather all necessary signatures.

The packet must be reviewed and approved by all appropriate authorizers prior to releasing data to the receiving party.

If the data to be released is to be extracted from Datatel/Coleague, the Business Systems team of Information Technology Services can assist you in defining the data to be extracted, including specific field names. They can also assist in identifying the specific records to be included in the extract.

Data cannot be released until the packet is fully completed and signed.

The Chief Information Officer will provide final approval and authorize the release of the data.

To Vendors:

Please use the checklist on Page 5 to guide you through the process. You are responsible for completing all of the questions in Section 2 of this document, gathering all related documentation, and returning the material to your client contact at the university.

To Approvers:

Please review the included material. After you have made a determination about whether you will approve the data release, please mark your decision on the signature sheet and return the entire packet to the CIO's office for final approval.

Data requesters, please use the following checklist to ensure that all requested items have been returned with your documentation.

- ☐ Section 1 has been completed by you
- ☐ A detailed and specific description of the data to be released has been developed, including the criteria that will be used to select the records to be released and the specific data fields to be included in the extract
- ☐ Section 2 has been completed by the vendor, returned to you, and attached
- ☐ All supplemental documentation provided by the vendor has been attached
- ☐ A copy of the contract with the vendor has been attached. NOTE: Where it is still under review, provide an unsigned copy of the proposed contract
- ☐ Return to the university's Information Security Officer for review. (ISO@regis.edu) The ISO will review and assess the materials, and then pass them on for signature or work with you to route for approval. (Please do not gather signatures yourself.)

Section 1

To Be Completed by Data Requestor (Regis University Representative)

Please provide answers to the following questions; please make your responses as detailed and specific as is reasonably possible.

1. Who is the requester of this data release (include name, department, title, and extension)?

_____.

2. What database is the source of the data? If the data resides on a departmental server or individual workstation, where is the server located? If no extract is required, where will the data to be stored on the vendor's systems come from?

_____.

3. Describe the reason for sending data to an outside vendor – what is the objective/goal of the use of the data?

_____.

4. As specifically as possible, what criteria will be used to select the records to send to the vendor? (e.g. all current students receiving financial aid)? Ignore if no data extract is required.

_____.

5. Please list the information components/database fields to be included in the extract (be as specific as possible, preferably including database field names or a database data map. For example: "Date of Birth" from SPBPERS_BIRTH_DATE). If no data extract is required, describe as specifically as possible the information that will be stored on the vendor's systems.

_____.

6. What is the term of the agreement? How long will the data be used/stored by the receiving party?

_____.

7. How frequently will the data need to be extracted and will the process need to be automated?

_____.

8. Who (please provide the name of a specific person or a specific role) will be responsible for maintaining and managing user accounts on the third-party system. This person/role must be responsible for managing access to the data on the third-party system, including creating, modifying, and deleting user accounts. This person/role may not delegate account management to another person/role and must ensure that other users who are given access to the data cannot extend or elevate their account access privileges.

_____.

9. Will the vendor be sending data back to the university as part of this process and will that data need to be processed by any university data systems such as Colleague/Datatel? Please describe as specifically as possible what data will be returned and what will be done with the data when it is received.

_____.

Vendors, please use the following checklist to ensure that all requested items have been returned with your documentation.

- ☐ Fully complete Section 2 of this document

If available, please attach copies of each of the following documents:

- ☐ A copy of the vendor's security policies
- ☐ A copy of the vendor's incident response plan
- ☐ A copy of the vendor's backup policies
- ☐ A copy of the vendor's data retention policies
- ☐ A copy of the vendor's privacy/data release policies
- ☐ A copy of the vendor's Voluntary Product Accessibility Template (VPAT) level.
    - If VPAT isn't finalized, then provide a copy of ADA Compliancy Project Plan
    - If ADA Compliancy Project Plan isn't available, explain ADA Compliancy Support (Minimum level is WCAG 2.0)
- ☐ A signed copy (by an authorized representative) of the incident notification agreement
- ☐ A certificate of insurance defining the vendor's coverage and levels for Technology Errors and Omissions (Technology E&O) insurance and listing Regis University as an insured
- ☐ A certificate of insurance defining the vendor's coverage and levels for Fidelity/Computer Crime insurance and listing Regis University as an insured
- ☐ A certificate of insurance defining the vendor's coverage and levels for General and Automobile Liability insurance and listing Regis University as an insured
- ☐ A summary/report of the vendor's most recent security audit (independent third-party)
- ☐ Documentation of compliance with PCI DSS (as appropriate)
- ☐ Documentation of compliance with HIPAA (as appropriate)

Section 2

To Be Completed by Vendor

1. Does your company have written data security policies? (If yes, please attach copies of all written data security policies.)

☐Yes ☐No

2. Does your company have written policies or response plans covering notification of the client in the event of an incident involving loss, release, or unauthorized access of client data? (If yes, please attach copies of these documents.)

☐Yes ☐No

3. Does your company have written data backup policies, procedures, or plans? (If yes, please include copies of these documents.)

☐Yes ☐No

4. Does your company have written policies regarding retention of client data? (If yes, please include copies of these documents.)

☐Yes ☐No

5. Does your retention plan include policies regarding disposition of client data following contract completion or termination? (If yes, please include copies of these materials.)

☐Yes ☐No

6. Does your retention plan address retention and disposition of client data on backup tapes or other media? (If yes, please include copies of these materials.)

☐Yes ☐No

7. Does your company have written privacy policies regarding client data? (If yes, please include copies of these documents.)

☐Yes ☐No

8. Is your company routinely audited by an independent, third-party security firm? (If yes, please include a copy of the most recent audit verification and results summary.)

☐Yes ☐No

9. Does your company carry Errors and Omissions (E&O) insurance for client data? (If yes, please include industry standard documentation of the insurance coverage describing the coverage type and limits.)

☐Yes ☐No

10. Does your company carry Fidelity/Computer Crime insurance for client data? (If yes, please include industry standard documentation of the insurance coverage describing the coverage type and limits.)

☐Yes ☐No

11. Does your company carry General and Auto Liability insurance? (If yes, please include documentation of the insurance coverage including a certificate of insurance describing the coverage type and limits.)

☐Yes ☐No

12. Will your company or a sub-contractor be processing credit card transactions on behalf of Regis University? (If yes, please include documentation of compliance with PCI DSS.)

☐Yes ☐No

13. Will your company or a sub-contractor be processing or storing personally identifiable medical records or medical information that may be subject to HIPAA regulation on behalf of Regis University? (If yes, please include documentation of compliance with HIPAA.)

☐Yes ☐No

14. Describe in detail how the data provided to you will be secured and protected. (Include information regarding physical security, security on systems storing or accessing client data, database security, encryption of data at rest and in motion, separation of duties, firewalls, and any other security measures used to protect client data.)

_____.

15. Following the termination/expiration of the agreement, how will the data be returned to Regis University and/or destroyed (include information regarding how backup tapes and other media will be identified and expunged?

_____.

16. How will the data be transferred between Regis University and your systems and what mechanisms will be used to secure the data during transport? (Include specific preferred protocols or security technologies, such as Secure FTP, PGP, etc.)

_____.

Authorizing Signatures

The signers below agree that they have reviewed the material in this data release packet and approve the release of the data as described in the packet.

I approve/ conditionally approve/do not approve this data release request.

_____

Area Vice President-Requester Date

_____

Area Vice President-Data Owner (If different) Date

_____

Risk Management Officer Date

_____

FERPA Compliance Officer (If necessary) Date

_____

Chief Information Officer Date

If you conditionally approve the request, please indicate the conditions that must be met for approval:

_____

_____

_____

_____

_____

_____

_____

_____