INFORMATION SECURITY REVIEW QUESTIONNAIRE

V1.2

This questionnaire facilitates the identification of security requirements for a CUNY information technology project, application or system. The questionnaire is intended for those CUNY projects, applications and systems that involve Non-Public University Information or that acquire ongoing vendor IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc.)

Introduction

Identifying information security requirements in the earliest planning stages of a technology project is important to reduce the risk of introducing new security issues into the University environment. Involving CUNY/CIS Information Security early on also minimizes potential project schedule delays when security requirements are retrofitted into systems and/or contractual agreements late in the process.

Name of Application: Click here to enter text.

1. **DATA CLASSIFICATION**

   Purpose *This section identifies the highest sensitivity level of data that the project involves. This information is needed to determine baseline data security requirements that must be addressed during the project.*

   1.1. The project involves: *(check all that apply)*

   ☐ Non-Public University Information

   Subcategories:

   ☐ Personally Identifiable Information

   ☐ Educational records and/or other information subject to FERPA regulations

   ☐ Information regarding an individual's mental or physical condition and/or history of health services use and/or other information subject to HIPAA regulations

   ☐ Financial information, including credit card and bank information, budgeting, salary and financial aid information

   ☐ Human Resources information

   ☐ Research information

   ☐ Other data the project sponsor considers sensitive, private, confidential or non-public

   If any box above is checked, explain the nature, type and quantity of the data and why the involvement of this non-public university data is essential to the system or service to be delivered by the project:

   Click here to enter text.

2.   USE OF VENDOR IT SERVICES

Purpose *This section describes the intent, if any, to acquire ongoing vendor IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc.) in support of this project or service. This information is needed to determine security requirements that should considered when evaluating vendor services and negotiating vendor contracts.*

2.1 Will the project acquire ongoing vendor IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc)?

☐　　　Yes

☐　　　No. If checked, skip to Section 3.

2.2 The vendor service(s) will be acquired via:

☐　　　Request For Proposal

☐　　　Sole Source Procurement

☐　　　Purchase Order

☐　　　Agreement to vendor's online license user agreement

☐　　　Other. If checked, describe here:

Click here to enter text.

2.3 Briefly describe below the service(s) to be acquired, including names of desired vendor(s) if known:

Click here to enter text.

3. Identity Management, Access Control, Authorization

Purpose

This section identifies the user population who will have access to the IT product or service to be delivered by the project, as well as planned security access controls. This information will help determine if additional controls are needed to reduce the risk of unauthorized or otherwise inappropriate access to sensitive data.

3.1. Who will access this application or system?

☐ Faculty

☐ Staff

☐ Students

☐ Consultants and temporary employees

☐ Other (please explain):

Click here to enter text.

3.2. If not covered above, what entities external to the University will have access to the application or service? Click here to enter text.

3.3. Is access limited to only those individuals whose job or function requires such access? Click here to enter text.

3.4. Is any part of the system open to the public or to an anonymous class of users? Click here to enter text.

3.5. Briefly describe the process by which authorization of users will likely be accomplished, if known. Click here to enter text.

3.6. Are there different levels of authorization in the system? (e.g., full access, limited access, read-only access, etc.) Click here to enter text.

3.7. Is there an identified authority that approves requests for access to this system? Who would that be? Click here to enter text.

3.8. Is there a process for the access administrator to be notified when a user's status or role changes? Click here to enter text.

3.9. Will there be uniquely identifiable accounts for all users requiring access? Click here to enter text.

3.10. How will accounts which are no longer needed be recognized and deleted in timely and manageable manner? Click here to enter text.

3.11. How will this system authenticate users?

☐   CUNY Portal LDAP Single-Sign On

☐   Active Directory (cuny.adlan)

☐   CUNY Enterprise Active Directory

☐   CUNYfirst Single-Sign On

☐   Local Authentication

☐   Other:

Click here to enter text.

3.12. Where local authentication is used, provide details on the enforced password complexity and expiration policy. Click here to enter text.

3.13. Where local authentication is used, provide details on how passwords are securely stored within the system (e.g., encrypted using a salted hash). Click here to enter text.

3.14. Does the application automatically log off, lock or terminate a session after a predetermined time of inactivity? Provide details. Click here to enter text.

4. Network Access and Communication

Purpose

This section identifies the scope of network access requirements. This information will help determine controls needed to reduce the risk of unauthorized or otherwise inappropriate access to sensitive data.

4.1. Is this system required to be network accessible? ☐ yes   ☐ no

4.2. If so, will it be accessible:

☐ only within CUNY Central Office networks

☐ only within one or more CUNY Campus networks (specify)

☐ both CUNY Central Office and CUNY Campus networks

☐ the Internet at large

☐ other – please explain:

Click here to enter text.

4.3. If available, provide a network diagram that depicts required connectivity for all of the components of the application or service.

4.4. Will this system be accessible through means other than the network (e.g., telephone)? Click here to enter text.

5. Data Protection

Purpose

This section identifies available data protections and requirements. This information will help determine controls needed to reduce the risk of unauthorized or otherwise inappropriate access to sensitive data.

5.1. Are there restrictions on what quantity or type of data can leave the system? Please explain. Yes, faculty/administrator users with the necessary access rights provided in the ExamSoft Portal can export the following – question content they have access to, exams, and exam specific data (student results, question performance, etc).

5.2. Are shadow copies of any of the data anticipated to be created? For example, would users copy or download data to their own devices? If so, please explain. No. Only your users who are granted the necessary access rights can manually export the above information.

5.3. Does data associated with this application or system interface with other applications or systems? If so, please provide details. No.

5.4. Is non-public university data encrypted while at rest? ExamSoft is an exam taking solution that utilizes an offline approach for examinations. By operating exams in an offline mode we increase the stability of our solution and eliminate many internet based stability and security risks for the exam taking experience. For our most sensitive data resource (exam files downloaded to the student device & answer files uploaded from the student) all data IS encrypted at rest and while in transit. Further we utilize SSL/HTTPS for all of our web-based systems to ensure that connections are encrypted while data is in transit

5.5. Is the data encrypted while transmitted over an untrusted network? Yes.

5.6. What type of encryption is used? How is it configured and deployed? TLS 2.0/SSL encryption, as well as proprietary encryption for all student exam and answer files.

6. **Logging and Auditing**

Purpose

This section identifies available activity logging and auditing capability. This information will help determine whether additional logging and auditing features needs to be established.

6.1. Describe logs and/or audit trails that are produced by the application or service. The entirety of the students experience and navigation while in the testing platform is logged, and viewable by your faculty/admin users who have the necessary permissions. User logs can be reviewed further via request to your dedicated Account Manager.

6.2. Is sensitive data embedded in the logs? No.

6.3. Can logs and/or audit trails link actions to individual users? Yes.

6.4. Are successful/unsuccessful accesses logged? With client network address? Yes.

6.5. For how long are logs retained? Student logs are not archived from the system and remain accessible to users with the necessary access rights.

7. Business Continuity / Disaster Recovery

Purpose

This section identifies business continuity and disaster recovery provisions and requirements.

7.1. Is there a documented business continuity / disaster recovery plan that addresses procedures to restore any lost data or functionality in the event of an emergency or other occurrence, the staff responsible for carrying out data restoration, emergency contact names and numbers, important business partners and other business supply information necessary for a temporary office setup to support data restoration?

Yes, ExamSoft has a documented business continuity/disaster recovery plan that is proven, reviewed, and tested on an annual basis.

8. Other Comments

Click here to enter text.