RIT | Information Security

ITS INFORMATION ACCESS AND PROTECTION QUESTIONNAIRE (IAPQ)

The purpose of this questionnaire is to help identify if an application or service involves private or confidential data, or performs a critical function for the institution which could negatively impact business operations. The ITS Information Access and Protection Questionnaire is used when a new application/service is planned or expected, or when a significant change to an existing application/service is expected. This questionnaire should be completed by the business unit with primary responsibilities for the application/service, and **a copy of this completed and signed questionnaire should be retained by both the business unit and ITS.**

The Information Access & Protection (IAP) Standard requires all departments (or higher level organizational units if uniformity allows) to identify and maintain an inventory of all private, confidential, and internal information they handle or maintain. This standard can be referenced at: https://www.rit.edu/security/content/information-access-protection-standard

The Solutions Life Cycle Management standard calls for only high impact services that store or provide access to Private or Confidential information, and/or support a Critical Business Process undergo technical security reviews. For additional information related to the categories of Private and Confidential Data, please see the Information Access & Protection Standard located at the following website: http://www.rit.edu/security/content/information-access-protection-standard

User Completing Questionnaire:	
Primary Business Process Owner:	
Primary ITS Contact Person:	
Solution Name:	
Brief Description of Solution:	
Type of Solution:	New Application/Service Existing Application/Service (change request)

Once completed, please signed and return this questionnaire to: **its_iapq@rit.edu.** The form will then be reviewed by ITS to determine if additional work will be necessary to ensure compliance with the RIT Solutions Life Cycle Management security standard: https://www.rit.edu/security/content/solutions-life-cycle-management

Section A: Information and Access Protection	Answer
Does\will this solution store or provide access to Social Security Numbers (SSNs), Individual Taxpayer Identification Numbers (ITINs), or other national identification numbers?	YES NO
If answer is YES please explain:	
Does\will this solution store or provide access to driver's license numbers?	YES NO
If answer is YES please explain:	
Does\will this solution store or provide access to financial account information (bank account numbers, checks, credit or debit card numbers), etc.?	YES NO
If answer is YES please explain:	
Does\will this solution store or provide access to employee or student health information as defined by the Health Insurance Portability and Accountability Act (HIPAA)?	YES NO
If answer is YES please explain:	
Does/will this solution store or provide access to educational records governed by FERPA that are not defined as directory information? See RIT Educational Records Policy D15.0: https://www.rit.edu/academicaffairs/policiesmanual/d150	YES NO
If answer is YES please explain:	
Does/will this solution store or provide access to faculty research or writing before publication or during the intellectual property period? See RIT Intellectual Property Policy 3.0: https://www.rit.edu/academicaffairs/policiesmanual/c030	YES NO
If answer is YES please explain:	
Does\will this solution store or provide access to University Identification Numbers (UIDs)?	YES NO
If answer is YES please explain:	
Does\will this solution store or provide access to employee personnel information?	YES NO
If answer is YES please explain:	

Does\will this solution store or provide access to management information designated as confidential?	YES NO
If answer is YES please explain:	
Does\will this solution store or provide access to faculty research?	YES NO
If answer is YES please explain:	
Does\will this solution store or provide access to third party information the RIT has agreed to hold confidential under contract?	YES NO
If answer is YES please explain:	

Based upon RIT's Disaster Recovery Security Standard.
https://www.rit.edu/security/content/disasterRecovery-HTMLStandard

[Critical]: Information or a process/function which if corrupted, lost, interrupted or made inaccessible during a disruption would pose a significant life, safety, financial, reputation, or other risk to RIT.

[Non-Critical]: Information or process/function which if corrupted, lost, interrupted or made inaccessible during a disruption would pose a minimal risk to RIT. The information or process/function could be supplied through alternate means during the disruption or delayed until after the disruption.

Section B: Business Impact	**Answer:**
Based upon the definitions above, does/will this solution support a **Critical** Business Process?	YES NO
Please explain:	

The accountability for all risk acceptance including IT risks is owned by the organizations within RIT that are creating and managing risks in relation to their operations. This document is intended to assist in that process by providing information for RIT Business leaders to use in making informed business decisions.

By signing this questionnaire you attest on behalf of your business unit that, to the best of your knowledge, the above answers are complete and accurate.

Acknowledgment by Primary Business Process Owner

Name: _____

Title: _____

Signature: _____ Date: _____