RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

Information Security Office
Division of the Office of Information Technology

INTRODUCTION:

The following questionnaire has been developed to assist departments evaluate the security/compliance of third parties or application service providers, for the protection and security of Rutgers University information assets and resources. The goal is to provide a safe environment for Rutgers University data and confidentiality for our clients.

The categories defined on this questionnaire are mapped to the ISO 27002:2013 Security Clauses.

The International Standard 27002 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The ISO 27002 provides general guidance on the commonly accepted goals of information security management. This standard serves as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

WHO SHOULD FILL THIS DOCUMENT:

GENERAL INFORMATION SECTION 1: Should be completed by the requester (Rutgers Staff)

GENERAL INFORMATION SECTION 2 and the rest of the Questionnaire should be completed by the vendor.

NOTE: This questionnaire will only be considered for review if all the questions have been addressed.

1	**General Information (to be filled out by the requester - Rutgers staff)**		
1.1	Date		
1.2	Rutgers Department and Contact Name		
1.3	Telephone #		
1.4	Rutgers Email		
1.5	Service/Application Name		
1.6	Please explain in detail: How does the Service/Application help the Business Unit/School to achieve its goals?		
1.7	Determine the Classification of Data that the service/application will manage, use, transmit, store, etc. (Use the *Data_Classif_Levels* tab to answer this question*)*	*Select the level*	
1.8	Based on the previous question, please provide examples of the type of data that the service/application will manage/store (such as PHI, PII, SSN, PCI-related data, research data, etc.)		
1.9	List the software interfaces of this solution/application (*- If this solution obtains information from other internal /external applications.* *- If this solution provides information to other internal /external applications*)		
1.10	Is Rutgers planning to de-identify ePHI data before uploading it to a third party application?	Select the answer:	Please use this space to provide more details
1.11	Will the vendor de-identify ePHI data?	Select the answer:	Please use this space to provide more details
1.12	If so, which HIPAA method do you use / does the vendor use to de-identify the data? (e.g. Safe Harbor or Expert Determination)		
1.13	Please provide /ask the vendor to provide copies of system architecture diagrams and data flow diagrams as they pertain to the service being provided. (See example of data flow diagram at the *Ex_Data_Workflow* tab)		

2	**General Information (to be filled out by the vendor)**		
2.1	Vendor Contact Name & Email		
2.2	Does your company have a position or organization responsible for overseeing the company's overall security program?	Select the answer:	Please use this space to provide more details
2.3	Please provide a detailed description of the Service/Application		
2.4	Describe what additional services Rutgers University will receive as part of this acquisition (e.g. implementation, maintenance, monitoring, etc.)		

2.5	Can this application/system be accessed via the internet?	Select the answer:	Please use this space to provide more details
2.6	Explain in detail under what type of scheme or model will the service/application be implemented? (Include all applicable) (e.g.: - Standalone application - Ready to install application - Software as a Service - Customizable package - Custom-made application - Web Application To be installed in: - On Rutgers premises - On third party premises - In the cloud (private cloud / public cloud) - Hybrid Combination)		
2.7	Does the application/service require any installation of software on user's PCs or mobile devices?	Select the answer:	Please use this space to provide more details
2.8	Does your company employ a single-tenant or multi-tenant environment?	Select the answer:	Please use this space to provide more details
2.9	Is the company outsourcing any portion of the contract?	Select the answer:	Please use this space to provide more details
2.10	Is there an agreement already signed with Rutgers University? (BAA, NDA or a Confidential Disclosure Agreement)	Select the answer:	Please use this space to provide more details
2.11	Is, or was, the company involved in any confidentiality breaches where notification was involved?	Select the answer:	Please use this space to provide more details
2.12	Does the company meet responsibility for compliance legislation (NJ ID Theft, etc.) and 3rd party requirements (HIPAA, GLBA, etc.).		

3-13	**Specific Information (to be filled out by the vendor)**		
3	**Policies and Standards**		
3.1	Does your organization have formal Information Security Policy? If so, please furnish a copy of your security policy and standards.	Select the answer:	Please use this space to provide more details
3.2	Does your organization have a Security Incident Response Policy?	Select the answer:	Please use this space to provide more details
3.3	Does your organization have an Acceptable/Responsible Use Policy?	Select the answer:	Please use this space to provide more details
3.4	Does your organization have a Privacy Policy?	Select the answer:	Please use this space to provide more details

3.5	Is there a documented process for reviewing the application/system's audit logs?	Select the answer:	Please use this space to provide more details
3.6	Do you have a documented and currently followed change management process?	Select the answer:	Please use this space to provide more details
3.7	Does the company have documented IT system maintenance standards and procedures?	Select the answer:	Please use this space to provide more details

4	**Access Control**		
4.1	Does the application support CAS Authentication Protocol or Shibboleth Authentication Protocol?	Select the answer:	Please use this space to provide more details
4.2	Please describe your company's process and current controls to grant, modify, review and, terminate user access to the solution/application offered.		
4.3	Can a Second Factor Authentication be used for this solution?	Select the answer:	Please use this space to provide more details
4.4	Does the solution require all users to have unique user account?	Select the answer:	Please use this space to provide more details
4.5	Password Complexity Policy:		
4.5a	Does the solution permit temporary passwords to be changed at the first log-on?	Select the answer:	Please use this space to provide more details
4.5b	Does the solution permit passwords to be changed at least every 90 days or based on the number of accesses?	Select the answer:	Please use this space to provide more details
4.5c	Does the solution permit passwords for privileged accounts to be changed at least every 60 days?	Select the answer:	Please use this space to provide more details
4.5d	Are passwords required to be at least eight (8) characters composed by a combination of alphabetic, upper and lower case characters, numbers, and special characters (or a combination of any three [3] of the above four [4] listed)?	Select the answer:	Please use this space to provide more details
4.6	Are the passwords and user id's encrypted in the database?	Select the answer:	Please use this space to provide more details
4.7	Does the application/system terminate user's session after a period of inactivity?	Select the answer:	Please use this space to provide more details
4.8	How does your company monitor privileged accounts for the solution offered?		

4.9	Are audit logs available that include all of the following: login, logout, actions performed, and source IP address?	Select the answer:	Please use this space to provide more details
4.10	Is the company able to identify unauthorized access for this solution? If so, how, and what determines notification of the unauthorized access? what situations are not (or cannot) be audited?	Select the answer:	Please use this space to provide more details
4.11	Are your systems accessed remotely? If so please describe security controls.	Select the answer:	Please use this space to provide more details
4.12	Does your company enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)? If so, please provide supporting documentation.	Select the answer:	Please use this space to provide more details
4.13	How does the company secure the network perimeter? (e.g. firewalls, IDS, IPS, etc.)		
4.14	How often are network perimeter logs reviewed?		
4.15	Does your company use dedicated secure networks to provide management access to your cloud service infrastructure?	Select the answer:	Please use this space to provide more details

5	**Exchange and Transport of Information**		
5.1	Please describe your company's process for secure exchange of electronic information.		
5.2	What protocols will be used to protect application data in transit (e.g., TLS, SSL, SFTP, FTP/S)? Please provide technical details, including version information.		
5.3	Does your company have security controls for email and Internet messaging (if allowed)? Please describe security controls.	Select the answer:	Please use this space to provide more details
5.4	Will your company permit University data to be transported outside of the company's central data stores (either to local clients or portable media)? What mechanisms are in place for this transport?	Select the answer:	Please use this space to provide more details
5.5	How is removable media controlled?		
5.6	Are laptops used to store or transport information? If so, how is it secured?	Select the answer:	Please use this space to provide more details
5.7	What processes does your company use to monitor the security of your wireless networks?		

5.8	How does your company monitor for unauthorized personnel, connections, devices, and software?		

6	**Confidentiality**		
6.1	Do your company's employees and third parties have privacy awareness and/or sign a nondisclosure agreement preventing them from disclosing confidential information?	Select the answer:	Please use this space to provide more details
6.2	Does your company do background checks on employees?	Select the answer:	Please use this space to provide more details

7	**Data Handling**		
7.1	Please describe the company's back-up process? How frequently is it tested?		
7.2	Is this solution part of the current back-up process?	Select the answer:	Please use this space to provide more details
7.3	How will your company secure University data in your backups?		
7.4	Are backups encrypted?	Select the answer:	Please use this space to provide more details
7.5	How data at rest is protected?		
7.6	What is the company's disaster recovery/business continuity policy & process? - How often is it tested? - Is any portion outsourced?		
7.7	Is this solution included in the current disaster recovery / business continuity plan?	Select the answer:	Please use this space to provide more details
7.8	Has the company activated all or part of your BCP/DRP in the last twelve (12) months? If yes, please describe the scenario and the impact it had on your ability to meet customer service commitments.	Select the answer:	Please use this space to provide more details
7.9	How is equipment being disposed of and stripped of data, prior to disposal according to regulations?		
7.10	Are backups and /or alternate copies destroyed as a part of the process?	Select the answer:	Please use this space to provide more details
7.11	Is sensitive information removed prior to equipment repair?	Select the answer:	Please use this space to provide more details

7.12	Does the company have a data retention policy? Will any information retained by company for their own purposes?	Select the answer:	Please use this space to provide more details
7.13	Will the company allow sharing or selling of any information collected, to other entities including government (i.e., subpoenas)? If so, what are the procedures?	Select the answer:	Please use this space to provide more details
7.14	How will Rutgers information be disposed of due to contract termination/cancellation, or if the information is no longer required?		

8	**Incident Response**		
8.1	Does the company have an incident response program?	Select the answer:	Please use this space to provide more details
8.2	How frequently does your company log and review security-related events?		
8.3	How quickly will Rutgers be notified in the event of an incident involving university information? What determines notification? Please specify whether or not the University will have an account-specific contact at your organization.		
8.4	Please describe (at a high level) the technical and operational controls your company has implemented to detect and respond to security events and incidents.		
8.5	What is your expected recovery time for the services provided to the University?		
8.6	If applicable, does the company have procedures in place to provide access to ePHI data during an emergency?	Select the answer:	Please use this space to provide more details

9	**Environment**		
9.1	How does your company control access to physical equipment?		
9.2	How are areas protected from natural & manmade disasters? (flooding, fire, etc.)		
9.3	Are areas protected from environmental hazards? (extreme heat, static electricity, etc.)	Select the answer:	Please use this space to provide more details
9.4	If the company stores university data on equipment outside of the company how is it controlled?		
9.5	Does your company outsource any IT or IT security functions to third party service providers? If so, who are they, what they do and, what type of access do they have?	Select the answer:	Please use this space to provide more details

9.6	Does your company rely on one or more cloud service providers? If so, please confirm which controls are maintained by your company and which controls are maintained by your provider (e.g., patch management, log management).	Select the answer:	Please use this space to provide more details

10	**Compliance and Audit**		
10.1	Does your company have a complete and successful SOC2 or SOC3 reports? If so, please provide your company's latest reports.	Select the answer:	Please use this space to provide more details
10.2	Does your organization have system and/or process certifications? If applicable, please provide current attestations. SSAE16/SysTrust HIPAA PCI DSS FERPA ISO 27001 NIST/FISMA Cloud Security Alliance (CSA) self assessment or CAIQ? Cloud Security Alliance STAR certification Data Privacy Policy Other (i.e., independent vulnerability assessments of your systems and/or applications)	Select the answer:	Please use this space to provide more details
10.3	Does your company have a process to address audit recommendations and to ensure compliance with security policies and standards?	Select the answer:	Please use this space to provide more details
10.4	Has a third party security review been performed by an external organizational? If so, please furnish the results.	Select the answer:	Please use this space to provide more details

11	**Security Testing**		
11.1	Does your company run and monitor a process to ensure that all systems are protected with the most updated virus protection software? Are users made aware of their responsibilities in preventing the spread of viruses and other malicious code?	Select the answer:	Please use this space to provide more details
11.2	Does your company have a process to identify and patch vulnerabilities affecting network infrastructure, applications, and operating systems in your environment? If so, please describe.	Select the answer:	Please use this space to provide more details
11.3	Does your company conduct penetration testing to assess the security of your perimeter network (e.g., firewall, routers, remote access servers, web applications)? If so, how often are tests conducted?	Select the answer:	Please use this space to provide more details

12	**System acquisition, development and maintenance**	
12.1	Describe the development language(s) (Java, .NET, iOS, etc.) the application was / will be developed with.	
12.2	Please provide details about the methodology that your company uses to develop software.	

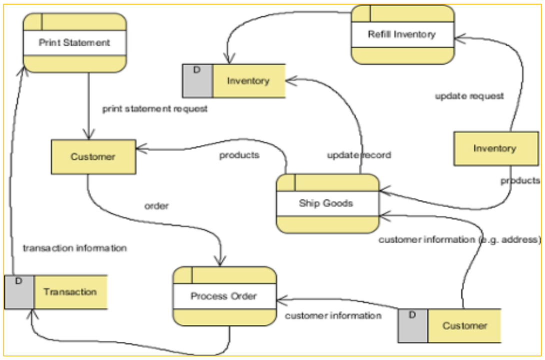
12.3	How does your company identify and validate the security requirements prior to the development and/or implementation of the information system?		
12.4	Does your company perform a security feature review (authentication, access controls, use of cryptography, etc.)?	Select the answer:	Please use this space to provide more details
12.5	How does your company implement data input and output integrity routines for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse?		
12.6	Does your company use non-production systems to prohibit the storage and use of production data in non-production (e.g., test and development) applications?	Select the answer:	Please use this space to provide more details
12.7	How does your company select and protect test data in the test/QA environment?		
12.8	Are testing procedures in place to determine whether security features are effective?	Select the answer:	Please use this space to provide more details
12.9	Does your company perform secure code reviews against the entire code base in the development phase?	Select the answer:	Please use this space to provide more details
12.10	Is there a security expert who performs the code review? (Describe who conducts the code review.)	Select the answer:	Please use this space to provide more details
12.11	Do all developers receive formal software security training?	Select the answer:	Please use this space to provide more details
12.12	Does your company use scanning tools against web apps during the QA phase?	Select the answer:	Please use this space to provide more details
12.13	Does your company use industry standards (e.g. OWASP for security applications) to validate security risks in applications?	Select the answer:	Please use this space to provide more details
12.14	How often does your company perform pen testing of applications (not perimeter pen testing)?		
12.15	Does your company outsource any development?	Select the answer:	Please use this space to provide more details

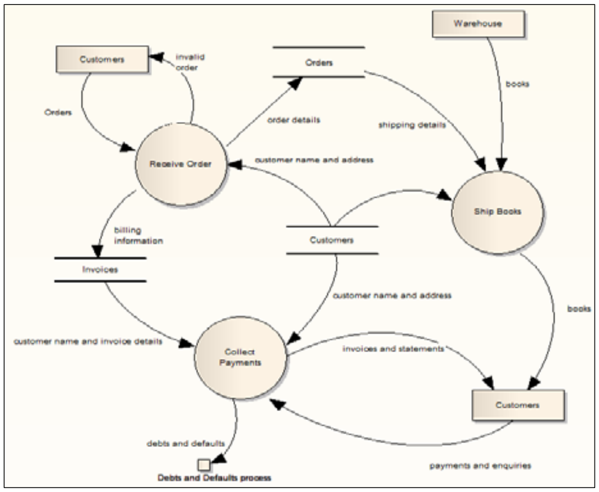
13	**Virtual Infrastructure**		
13.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Select the answer:	
13.2	If using virtual infrastructure, does your company provide tenants with a capability to restore a Virtual Machine to a previous state in time?	Select the answer:	

13.3	If using virtual infrastructure, does your company allow virtual machine images to be downloaded and ported to a new cloud provider?	Select the answer:	
13.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	Select the answer:	
13.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	Select the answer:	

Data Classification Level	Type	Examples (include, but are not limited to)
Restricted Data	ePHI - Electronic Protected Health Information - HIPAA	The following individually identifiable data elements, when combine with health information about that person, make such PHI: - Names - Address - Birth Date - Telephone numbers - Vehicle identifiers and serial numbers, including license plate numbers - Fax numbers - Email addresses - URLs - Social security numbers - Internet Protocol (IP) addresses - Medical record numbers - Biometric identifiers, including finger and voice prints - Health plan beneficiary numbers - Full-face photographs and any comparable images - Account numbers - Any other unique identifying number, characteristic, or code, except that allows identification of an individual
Restricted Data	Protected Data Related to Research	- Data containing sensitive information about human subjects
Restricted Data	Personally Identifiable Information - PII	- Social Security number, full and truncated - Driver's license and other government identification numbers - Citizenship, legal status, gender, race/ethnicity - Birth date, place of birth - Home and personal cell telephone numbers - Personal email address, mailing and home address - Religious preference - Security clearance - Spouse information, marital status, child information, emergency contact information - Financial information (salary, tax information, bank and debit/credit card numbers), - medical information, disability information - Law enforcement information, employment information, educational information - Military records - Biometrics
Restricted Data	Credit Card or Personal Credit Information - PCI-DSS	- Credit/Debit Card Number - Credit/Debit Card account Number, expiration date, verification Number, security code
Restricted Data	Student Education Records - FERPA	- Student Transcripts and grades - Student Disciplinary, or Judicial Action Information - Degree Information - Class Schedule - Advising Records - Other non-directory Information
Restricted Data	Student Loan Application Data - GLBA	- Student Loan Information - Student Financial Aid and grant Information - Payment History
Restricted Data	Other restricted information that University is required to protect under regulatory or legal requirements	- Institutional financial records - Individual donor information - Police Records
Internal Data	All other non-public information not included in the Restricted category	- University Identification / Information Number (employee ID, Student ID) - Rutgers University Policies - Authenticated portions of any rutgers.edu site
Public Data	Student Directory Information *- This data is not regulated by FERPA, can be released by the University without the student's permission. Students can request non-disclosure from the Rutgers Public Directory.*	- Student e-mail address
Public Data	Non-sensitive PII data disclosed from the Rugers Public Directory	- Office location - University's telephone number - University's email address - Other information that is released to the public

EXAMPLE OF DATA WORKFLOW DIAGRAM


Print Statement
Refill Inventory
D
Inventory
print statement request
update request
Customer
products
update record
Inventory
Ship Goods
products
order
customer information (e.g. address)
transaction information
D
Transaction
Process Order
customer information
D
Customer


Warehouse
Customers
invalid order
Orders
books
Orders
order details
shipping details
Receive Order
customer name and address
billing information
Customers
Ship Books
Invoices
customer name and address
books
customer name and invoice details
Collect Payments
invoices and statements
Customers
debts and defaults
payments and enquiries
Debts and Defaults process