Third Party/Vendor Data Security Assurance Questionnaire (SAQ)

Restricted Information (RI) When Filled In

Instructions for the Third Party Vendor/Organization:

Please respond to each question with a Yes, No, or N/A in the response box. If responding with a No or N/A, please provide additional information in the comments field.

#	Item	Response (Y/N/NA)	Comments	Feedback/Review (ISO use)
	Policies and Procedures			
A1	Is a senior official or officer within the organization directly responsible for the oversight and implementation of the security policies? If yes, please provide Title and contact information.			
A2	Does the organization employ procedures to ensure compliance with privacy laws and regulation requirements related to maintaining security, confidentiality, and protection of third party personal information? (e.g., Information pertaining to customers' employees, customers and/or producers)			
A3	Can the organization submit documents proving it maintains liability insurance and preferably cyber risk insurance?			
A4	Does the organization publish and enforce security policy document(s)? Are these signed by your employees?			
A5	Does the organization communicate these procedures to subcontractors who may have access to customer data?			
A6	Does the organization monitor these procedures? *If yes, please explain in the comments field.*			
A7	Does the organization update standards, policies, and procedures frequently?			
	Does the organization have staff assigned to the following:			
A8	Security Awareness? If yes, please provide Title and contact information.			
A9	Policy Enforcement? If yes, please provide Title and contact information.			
A10	Risk Evaluation? If yes, please provide Title and contact information.			

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

A11	Risk Mitigation? If yes, please provide Title and contact information.			
A12	Regulatory Compliance? If yes, please provide Title and contact information.			
	Does the organization have standards, policies, and procedures covering the following:			
A13	HR practices?			
A14	Authorized/acceptable use of networked services?			
A15	Use of corporate email, intranet, and internet?			
A16	Password management?			
A17	Software/hardware acquisition?			
A18	Change management?			
A19	Encryption policy and standards?			
A20	Security related incidence response handling?			
A21	Data Handling Policy (to include data use, storage, and destruction of sensitive data)?			
A22	Third party access & remote access?			
A23	Is all security management functionality performed within the organization? *If No, meaning the organization outsources some or all of its security functionality, please explain in the comments field.*			
A24	Does the organization clearly document the consequences of policy non-compliance?			
A25	Does the organization perform background checks on employees?			
	Disaster Recovery and Business Continuity			
B1	Does the organization have a Disaster Recovery and/or Business Continuity Plan?			
B2	Does the organization test its recovery plans? *If yes, please respond how often in the comments field.*			
B3	When was the last time the organization conducted a test? *Please respond in comments field.*			
B4	What type of testing does the organization conduct? (e.g., Paper walkthrough, simulation drills) *Please respond in comments field.*			
B5	Does the organization test the recovery procedures for efficacy?			

B6	Does the organization document and practice manual backup/restore procedures in case of automatic backup failures?			
B7	Is the organization willing to permit UCF to participate in the recovery process to ensure we can establish connectivity and access systems at the recovery site?			
B8	How long does the organization estimate it will take to restore product or services should a serious business interruption occur? (e.g., Interruption that lasts more than one business day) *Please respond in comments field.*			
B9	How does the organization define "uptime" and "downtime"? (e.g., Is the system down if more than 5% of users are affected? Is the system "down" if it is so slow users cannot function regardless if they can login?) *Please respond in the comments section.*			
B10	Can the organization meet recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for all products and services contracted with UCF?			
B11	Did the organization base the above estimate on previous test results of the recovery plans? *If no, please explain in the comments field.*			
B12	Does the organization have pre-arranged recovery locations? *If yes, please list in the comments field.*			
B13	Are the organization's physical servers that will provide the services for UCF under a current support/warranty plan?			
B14	Does the organization include force majeure (outside the control of the organization) events in its SLAs? How does the organization define "Acts of God" *Please respond in the comments field.*			
	Physical Infrastructure Security			
C1	Does the organization own their own data center?			
C2	Where are the data center(s) located?			
	Does the organization employ the following physical security /perimeter control(s) in the data center?			
C3	Security Guards or Gate Keeper?			
C4	Operation Staff on premises 24/7?			
C5	Keys/Tokens/Cards?			
C6	Key Pad Controls?			

C7	Man Trap?			
C8	Biometric Controls?			
C9	Entry/Security alarm connected to the door that is capable of calling or notifying the proper personnel?			
C10	Motion triggered security cameras that record for at least fifteen days?			
C11	Employee identification cards or badges?			
C12	Locked storage areas to store user personal information?			
C13	Visitor identification cards or badges?			
C14	Does the organization monitor/log all access to data center?			
C15	Does the organization maintain visitor logs for more than 30 days?			
C16	Does the organization monitor and escort visitors through sections of its facilities?			
C17	Does the organization have redundant public utilities connections?			
C18	Does the organization employ adequate surge protected Uninterrupted Power Supplies (UPS), battery banks, generators, etc.? *Please explain in the comments field.*			
C19	Does the organization employ fire/flood detection and suppression systems that strive to minimize damage to the information resources they protect?			
C20	Can the organization provide a recent Service Organization Control (SOC 3) report, ISO 27001, ISO 27018 report or any other industry recognized audit report? If Yes, Please provide a copy.			
C21	If the report is something other than a (SOC 3) or ISO 27001 report, what is the scope and frequency of the audit?			
C22	Does the organization limit administrator level access on network and systems infrastructure to system administrators only? *Please define system administrator in the comments field.*			
C23	Is access to security logs strictly controlled? (firewall logs, etc.)			
C24	Does the organization have policies in place preventing employees from copying client data to mobile devices, external media, or forwarding it to third party email?			
C25	Does the organization have data loss protection tools in place to enforce the policy above?			

C26	Does the organization properly secure offices and/or work areas where sensitive data or systems reside during non-business hours?			
	Data Security			
D1	Will the organization guarantee UCF data to remain permanently owned by UCF?			
D2	Upon contract termination, when and how would UCF data return and or destruction will occur?			
D3	Who will have access to UCF data? Please respond in the comments field.			
D4	Is UCF data (account information or user files) ever on desktop/laptop or removable media?			
D5	How does the organization prevent other clients from accessing UCF data? *Please respond in comments field.*			
D6	Can the organization meet UCF's requirement to encrypt access credentials when passing them through a public network? *Please describe in the comments field.*			
D7	Will the organization encrypt UCF Data at Rest?			
D8	Does the organization employ mechanisms that facilitate secure data exchange such as SSL, TLS, SFTP, VPN, etc.? *Please explain in the comments field.*			
D9	Does the organization employ a "Default Deny" for all data except where UCF explicitly grants access?			
D10	Will the organization guarantee to UCF that it will not to store UCF data of any kind in a restricted foreign country?			
	Identity & Access Management			
	Identities			
E1	Will each user have a unique userid?			
E2	Will userids assigned by the service provider match UCF userids?			

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

E3	How and where does the organization store user IDs and Passwords? How does the organization secure the information and what type of encryption is used? (e.g., Active Directory) *Please respond in the comments field.*			
	Authentication			
E4	What user authentication methods does the hosted service support? *Please specify in the comments section.*			
E5	Does the organization maintain a password policy equal to or better than the UCF password standards? http://www.cst.ucf.edu/about/information-security-office/iso-resources-rewrite/strong-passwords-at-ucf/			
E6	Will authentication rely on UCF systems?			
E7	Does the organization support authentication methods such as Federation (SAML compliant) or Single Sign On? *Please explain in the comments section.*			
E8	Does the hosting service provide authentication mechanisms?			
E9	Can the service provider's system be configured to require strong passwords?			
E10	Can UCF dictate password criteria as needed to ensure compliance with UCF security standards?			
E11	Can the service provider's system be configured to expire user passwords periodically in accordance with UCF security standards?			
E12	Does the service provider offer users secure self-password reset capabilities?			
E13	Does the service provider offer administrators and/or help desk staff a dashboard and/or API to administratively reset user passwords?			
E14	Can the service provider lock accounts after a UCF defined number of unsuccessful login attempts?			
E15	Are passwords entered in a non-display (masked) field?			
E16	Can the service provider meet UCF's requirement to encrypt all passwords during network transit?			
E17	Are passwords encrypted in storage? *(If yes, please explain in the comments field.*			

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

	Authorization			
E18	How will authorization controls be maintained? *Please explain in the comments section.*			
E19	Can the service provider configure authorization process controls to automatically disable user accounts or access privileges after a UCF defined period of non-use?			
E20	Can the service provider's system deauthenticate users after a UCF defined period of inactivity?			
E21	Does the service provider's system offer the ability to restrict access within the application based on roles assigned to authorized users?			
	Accounting			
E22	Can the service provider's security controls detect and report unauthorized access attempts?			
E23	Are all attempted and successful logins logged, include date/time, userid, source network address, and maintained for at least one year?			
E24	Will the service provider's system provide easy to read security reports that identify users and their access levels for periodic review?			
E25	Does the organization support account lockout policies on their customer's hosted site?			
	Incident Response			
F1	Are security incidents monitored and tracked until resolved?			
F2	Does the organization have a breach response plan that includes notifying customers if sensitive data is unknowingly or accidently released?			
F3	Is incident information and common vulnerabilities or threats shared with data hosting customers?			
F4	Will a third party ever have access to the service provider's hardware or systems that store UCF's Restricted Data?			
F5	Are the service provider's database and web server access and error logs regularly reviewed for anomalies that could indicate a compromise?			

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

F6	What process does the service provider have in place to identify security breaches on vendor managed systems (e.g., file integrity checks)? *Please explain in the comments field.*			
F7	In the case of a security breach or unexpected exposure of UCF Restricted Data, what are the hosting service provider's incident response procedures? *Please explain in the comments field.*			
F8	What is the service provider's process for disclosing to UCF any data requests, such as subpoenas or warrants, from a third party? *Please explain in the comments field.*			
F9	Has the organization ever experienced a breach of customer data? *If yes, please explain the extent of the breach and the controls implemented to prevent future breaches in the comments field.*			
F10	Does the organization employ procedures to comply with Florida's data breach notification law? *(If no, please explain in the comments field)*			
F11	Will the organization reimburse UCF for any expenses related to a data breach where the "at fault" party was not UCF (UCF did not cause the data breach)?			
	Patch Management			
G1	Does the organization review, test, and apply software patches on a regular basis?			
G2	Does the organization have an automated patch management solution deployed? *If no, please explain in the comments field.*			
G3	Does the organization review, test, and apply updates to server firmware (e.g., bios, raid card) and other appliance firmware on a regular basis?			
	Network Infrastructure			
H1	Does the organization maintain up-to-date network infrastructure and administration procedures?			
H2	Does the organization have perimeter scanning/monitoring agreements with managed network services providers?			

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

H3	Does the organization configure all routers with access control lists to allow only specific traffic to pass through?			
H4	Does the organization secure administrative access to its routers and console ports?			
H5	Does the organization have a procedure to track vulnerability patches for networking devices?			
H6	Are all networking devices at the latest patch level? *If no, please explain in the comments field.*			
H7	Does the organization change all default passwords on networking devices?			
H8	Does the organization control the change frequency and distribution of admin access to network infrastructure?			
H9	Does the organization use 802.1x complaint security for the wireless network? If yes, what vendor and type (e.g., none, WEP, WPA, WPA2)?			
	Which of the following intrusion prevention/detection systems does the organization employ:			
H10	Host-based Intrusion Detection Systems? (HIDS)			
H11	Network Intrusion Detection/Prevention System? (NIDS)			
H12	Rogue device and network anomaly detection? *If yes, please explain in the comments field.*			
H13	Does the organization monitor security policy violations and application/ networked services availability?			
H14	Does the organization log account success and failures events?			
H15	(If YES to H14) Is there a process in place to review the log data and address anomalies?			
	Application Security			
I1	What software development life-cycle methodologies does the hosting service provider use in the development of their software (e.g., TSP-Secure, SAMM, Microsoft SDL, OWASP, NIST SP800-64 rev 2,)? *If yes, please explain in the comments field.*			
I2	Are security components identified during each phase of the software development life -cycle?			

I3	Does the service provider have change management policies in place?			
I4	Are customers notified of changes? *If yes, please explain how in the comments field.*			
I5	Will the hosting service provider provide UCF lead-time for upcoming changes? *If yes, please specify how much lead-time in the comments field.*			
I6	Does the hosting service provider regularly perform source code audits?			
I7	Are source code audits performed by someone other than the person or team that wrote the code?			
I8	Does the service provider perform periodic Application penetration testing?			
	Remote Access and VPN			
	Are there any remote access/remote control methods available to access the organization's network, as follows:			
J1	RADIUS?			
J2	User ID/Password?			
J3	Other? – *If yes, please explain in the comments field.*			
J4	Does the organization force performing supervisory or administrative functions over encrypted external links? *If no, please explain in the comments field.*			
J5	Does the organization collect and review remote access audit log data?			
	Firewall			
K1	Does the organization employ firewall services to protect the network?			
K2	Is the organization's firewall installed on a dedicated system and is it kept up-to-date? *If no, please explain in the comments field.*			
K3	Does the organization allow non-standard (>1024) IP ports to pass through the firewall? *If yes, please explain in the comments field.*			

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

K4	Does the organization regularly scan and verify all the allowable services provided by the firewall server?			
K5	Does the organization use firewall-reporting tools to analyze the firewall log?			
K6	Does the organization periodically document and verify security policies on the firewall?			
K7	Does the organization protect internal IP address range(s)? (e.g., use NAT/RFC 1918)			
	Malware Controls			
L1	Does the organization scan all emails for malware?			
L2	Is there explicit policy requiring anti-malware software on networked computers?			
L3	Does the organization have centralized administration of malware control, such as distribution of signature updates, reporting, policy enforcement, and vendor management?			
L4	Are additional measures in place to protect against malware? *If yes, please explain in the comments field.*			
L5	Does the malware checking software run in the background with established frequency of scanning, etc.?			
L6	Does the organization prevent end-users from disabling malware protection software?			
L7	Does the organization allow installation of personal and non-corporate software or hardware on network computers? *If yes, please explain in the comments field.*			
L8	Does the organization employ Application Whitelisting to ensure non-approved programs such as malware cannot execute on managed workstations?			

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

Authorization and Signature Page

Print Name of Organization Official: _____

Signature of Organization Official: _____
(Signature) (Date)

Print Name of College/Departmental Security Coordinator (DSC): _____

Signature of College/Departmental Security Coordinator (DSC): _____
(Signature) (Date)

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution