Subject:	Vendor Risk Management Standards
Standards Number:	120
Effective Date:	August 9, 2019
Revised Date:	
Responsible Authority:	Information Security Office
Pages:	9

ACCOUNTABILITY:

Any UCF faculty and staff involved with the evaluation, procurement, implementation, and maintenance of third party systems and engagements are responsible for following the standard.

All UCF units should work to move towards compliance with the standard on an ongoing basis, not only during the procurement phase of a particular vendor. Units should consider a periodic review of all the vendors that process their data to ensure the vendors are meeting these standards.

APPLICABILITY:

This standard applies to any third party or vendor that may have access to, store, transmit, process, or collect any UCF data on our behalf. If any of the following statements are true, these standards apply:

- If you are transferring data currently residing on a computer system owned by the University of Central Florida to a computer system not owned by the University of Central Florida.
- If you are contracting with a service provider who will create a web site or implement a system on behalf of the University of Central Florida to collect, process, or store university data.
- If you are contracting with a service provider to collect data that will later be transmitted for use by the University of Central Florida.
- If you are contracting with a service provider that will accept credit card payments on behalf of the University of Central Florida.

If you have any questions about the applicability of the Vendor Risk Management process, contact the Information Security Office.

STANDARDS STATEMENT:

The purpose of this document is to establish minimum-security standards for the review and implementation of third party systems. They should be applied to all university third-party vendors and service providers in order to maintain the confidentiality, integrity, and availability of university data.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

STANDARDS

In the Tables below, an 'X' indicates a requirement to implement the given security control if the corresponding data type is present on the system.

Definitions and examples of Unrestricted, Restricted, and Highly Restricted Data can be found in UCF Policy 4-008 at https://policies.ucf.edu/ .

See Appendix A for requirements that apply only to engagements where **only** Unrestricted Data is involved.

Section 1: Review Requirements					
#	Name	Requirement	Data Classification		
			Unrestricted	Restricted	Highly Restricted
1.1	Avoid Duplication	Prior to engaging a vendor, UCF units should consult the Vendor Inventory list to see if there is an existing solution for the use case that meets these standards and is already in use at UCF. The vendor inventory can be found at https://infosec.ucf.edu/vrm/ ***Note:*** *If vendor has been approved, but a different product from the same vendor requested has not, a VRM review may be required based on classification of data shared.*	**X**	**X**	**X**
1.2	VRM Assessment Report	Vendor must be reviewed by the Information Security Office (or designee). The resulting VRM assessment report, which contains identified risks and recommendations, must be signed by the appropriate university leadership. ***Note:*** *any vendors that process only Unrestricted Data do not require an assessment report, however units must follow these standards as well as the requirements in Appendix A.*		**X**	**X**
1.3	Vendor Inventory	All vendors that meet these standards should be added to the vendor inventory. The vendor inventory can be found at https://infosec.ucf.edu/vrm/ ***Note:*** *UCF unit should report any vendor that processes Unrestricted Data, as no formal assessment report is required, to be added to the inventory list. Vendor information should be supplied to infosec@ucf.edu in order to update the records as ISO manages the inventory list.*	**X**	**X**	**X**

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

1.4	Re-assessment	Vendors must be resubmitted to the Information Security Office to determine the applicability of a re-assessment in case of the following: • Any time the contract or agreement is changed or is up for renewal • Any time the data that will be shared with the vendor changes (especially if the newly proposed data is classified at a higher level of restriction) • Any time the means of data transfer changes, such as adding a connection to an on-premise UCF system • Any time the vendor experiences a data- or security-related breach, regardless if UCF data is involved in the breach.		**X**	**X**

Section 2: Documentation Requirements

What documentation needs to be submitted and reviewed?

#	Name	Requirement	Data Classification		
			Unrestricted	**Restricted**	**Highly Restricted**
2.1	HECVAT	Vendor must respond to the industry-standard "Higher Education Cloud Vendor Assessment Tool" security questionnaire. A link to the HECVAT can be found at https://infosec.ucf.edu/vrm/ ***Note:*** *a HECVAT may be requested for vendors processing Restricted Data if additional review or security assurance is needed.*			**X**
2.2	UCF Integrations Questionnaire	Vendor must respond to UCF's "Integrations Questionnaire", which contains security-related questions regarding identity and access management, data transfer, and integrations with existing UCF systems. A link to the UCF Integrations Questionnaire can be found at https://infosec.ucf.edu/vrm/		**X**	**X**
2.3	Industry-Standard Audit Report	Vendor must provide an audit report from an industry-standard, independent audit, such as a SOC2 Type 2, ISO27001, NIST 800-171 or other similar audit, performed within the last 12 months.			**X**
2.4	Proof of Cybersecurity Insurance	Vendor must provide a certificate stating that they carry cyber liability insurance.			**X**
2.5	PCI Documentation	If Vendor is identified as a PCI third party service provider (TPSP), the vendor must provide: • PCI Attestation of Compliance (AoC) • Responsibility Matrix Additionally, a Cardholder Data diagram may be needed upon request.			**X**

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

Section 3: Legal Requirements *What is required to be included in any contracts and agreements?*					
#	**Name**	**Requirement**	**Data Classification**		
			Unrestricted	**Restricted**	**Highly Restricted**
3.1	Mutually Executed Agreement	The engagement should be covered by a mutually executed (signed by both parties) agreement or contract. **Click Through Agreements**: If Restricted data or Highly Restricted data is involved, a click through agreement alone is not acceptable. Instead, engage the vendor to create a formal, mutually executed (signed by both parties) agreement. NO contract involving Restricted or Highly Restricted data shall be executed until an acceptable agreement has been negotiated between UCF and the other party/vendor, reviewed and approved by the UCF General Counsel's Office,		**X**	**X**
3.2	*Secure Handling of UCF Data* agreement	The *Secure Handling of UCF Data* Agreement must be signed by the vendor and included in the final set of agreements. Any edits or redlines to the "Secure Handling of UCF Data" Agreement, or any data or security-related edits to the contract in general, must be jointly reviewed by UCF Infosec and the UCF General Counsel's Office prior to acceptance and execution. In cases where there is no formal agreement (such as only having a PO), the "Secure Handling of UCF" Agreement must be executed and attached.		**X**	**X**
3.3	HIPAA Business Associates Agreement (BAA)	If Vendor is provided potential access to any data defined as Protected Health Information (PHI) under HIPAA and the Vendor meets the definition of a business associate under HIPAA, the Vendor is required to enter into a Business Associates Agreement with UCF. This BAA is in addition to the requirement in 2.2.			**X**
3.4	PCI Addendum	If Vendor is identified as a PCI third party service provider (TPSP), UCF requires that the Vendor must also agree to UCF's PCI Addendum. This PCI addendum is in addition to the requirement in 2.2.			**X**
3.5	GDPR	If the vendor processes personal information subject to the EU General Data Protection Regulation, the vendor must also agree to UCF's Data Protection Addendum (DPA). This addendum is in addition to the requirement in 2.2.	**X**	**X**	**X**

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

Section 4: Identity and Access Management (IAM) Requirements					
#	Name	Requirement	Data Classification		
			Unrestricted	Restricted	Highly Restricted
4.1	Federation	Implement federation so that UCF credentials can be used for authentication. *[1]Local Accounts are only acceptable for unrestricted data when federation is not available. (see appendix B for local account standards when this is the case)*	**X[1]**	**X**	**X**
4.2	Multi-Factor Authentication (MFA)	Implement multi-factor authentication (MFA) to add an additional layer of authentication to access the system. *[1]**Restricted Data:** Multi-Factor Authentication is required for administrative and power users of the system, but recommended for all accounts.*		**X[1]**	**X**
4.3	Account Management	User access must be managed by the UCF unit. People and processes must be in place to: i. Authorize and de-authorize users to the systems. ii. Perform regular reviews of users' access to the system.	**X**	**X**	**X**

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

Section 5: Data Exchange and Integrations					
#	Name	Requirement	Data Classification		
			Unrestricted	Restricted	Highly Restricted
5.1	Data Exchange	Integration(s) with on premise systems should meet *UCF Standard 108: File Transfer and Integrations Standards*	**X**	**X**	**X**
5.2	Mass/Automated Email	If vendor, solution, or business unit sends automated and/or mass email communications to end users, they should follow UCF Infosec's *Mass Email Guidelines*, located at: https://infosec.ucf.edu/awareness/mass-email-guidelines/.	**X**	**X**	**X**

Section 6: Data Management					
#	Name	Requirement	Data Classification		
			Unrestricted	Restricted	Highly Restricted
6.1	Limiting Data Involved	The UCF unit should ensure the data being requested by the system and uploaded by the users is consistent with the classification of data intended for the system.	**X**	**X**	**X**
6.2	Data Retention	Vendor's solution should be configured to purge data on a regular basis that meets the business needs of the business unit (such as at the end of each semester, or after a year of inactivity).	**X**	**X**	**X**
6.3	End of Agreement Data Handling	UCF unit must verify data is purged from vendor's systems after termination of agreement and must request a certificate of destruction (see section 3.x of *secure Handling of UCF Data* agreement)	**X**	**X**	**X**

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

Appendix A:

All of the requirements in this section only apply to engagements where the UCF unit has determined that ONLY unrestricted data will be involved. They are in addition to any requirements that apply to Unrestricted Data in the tables above.

Legal Requirements

UCF unit must review the agreement and ensure it contains the following data security language:

i. **Data Re-Use:** Agreement must state that UCF data must only be used for the intended purposes outlined in the agreement and not shared with any third parties. See *Secure Handling of UCF Data Agreement* section 3.2 for example language.
ii. **End of Agreement Data Handling:** Agreement must state that at the end of the agreement, data will be returned to the UCF unit and purged from the vendor's infrastructure. See *Secure Handling of UCF Data* section 3.6 for example language.
iii. **Data Breach:** Agreement must state that vendor agrees to notify the UCF unit and the UCF Security Incident Response Team (SIRT@ucf.edu) in the event of a breach of UCF data.
iv. **FERPA:** Agreement must state that the vendor agrees to comply with FERPA regulations when processing data classified as "Directory Information" under FERPA. See *Secure Handling of UCF Data* section 4.2 for example language.
v. **GDPR:** Agreement must state that the vendor agrees to comply with GDPR regulations when processing personal data subject to GDPR.

Data Management

UCF unit must ensure the solution does not request from users, input, or generate any data that could be Restricted or Highly Restricted.

- UCF unit must inform users that it is not acceptable to submit restricted or highly restricted data to this vendor.
- For a system used by students, do not prompt users to enter FERPA educational records or PII, or provide feedback on their work within the tool.
- Do not identify users based on their UCF NID, which is classified as restricted data. Use UCF ID instead.

End User Awareness and Account Management best practices when use of a vendor is optional

The following recommendations only apply if the following are true:

The end user self-enrolls in the tool (e.g. the UCF unit does not create a user account for them)
End-user use of a tool is optional (e.g. not required for coursework)
The UCF unit is not sending data to the vendor on the user's behalf, without their consent
The data being provided is not Restricted or Highly Restricted Data

1. UCF Unit must clearly communicate to end users that they are submitting information to a third party and they do so at their own risk.
2. UCF Unit must encourage end users to do the following:
    a. Read any pertinent terms of service, privacy policy, acceptable usage policies, etc.
    b. Do not submit any sensitive information
    c. Delete their account once it is no longer needed.

Appendix B: Local Accounts

The use of vendor-based local accounts is never recommended and not acceptable for solutions that process Restricted or Highly Restricted data. However, in cases where only Unrestricted Data is involved and an exception is made, follow these standards:

i. The local accounts must meet our Password Standards outlined in UCF Standard 501: Password Standards: https://infosec.ucf.edu/policiesandstandards/
ii. UCF unit should instruct users to use a separate password than the user's NID.
iii. Allow all users to opt into using Multi-Factor Authentication when possible (do not disable the feature)

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

DEFINITIONS:

BAA: Business Associate Agreement. An agreement between a healthcare entity and a contractor that defines the parameters in the use, handling, protection and responsibility of Protected Health Information (PHI).

CUI: Controlled Unclassified Information. Unclassified information requiring protection as identified in a law, regulation, or government-wide policy.

GDPR: General Data Protection Regulation. A legal framework consisting of guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

Federation: An implementation of standards/protocols to manage user identities across organizations via trust relationships.

HECVAT: Higher Education Cloud Vendor Assessment Tool. A matrix providing generalized security and data protection questions and issues regarding cloud services for consistency and ease of use.

HIPAA: The Health Insurance Portability and Accountability Act of 1996. HIPAA protects the security of individually identifiable health information.

ISO27001: A specification for an information security management system containing frameworks of policies and procedures regarding a vendor's risk management process.

MFA: Multi-factor Authentication. A method of authentication in which requires the user to provide at least two forms of identity validation before authorization is approved.

NIST800-171: A set of standards defining strategies to address security threats and vulnerabilities in computers/network infrastructures to safeguard CUI in nonfederal systems/organizations.

PCI: Payment Card Industry. Relevant to any vendors that process payments or credit card information.

Security information and event management (SIEM): A security tool that provides real-time monitoring, correlation of events, and notifications.

SOC2/3: A report generated by an independent auditor intended to provide assurance on a vendor's internal security posture. SOC2 reports are intended for consumption by clients of a product. SOC3 reports are typically used for marketing and are more generalized.

Vendor: Any third party, service provider, or an entity that is not directly affiliated with UCF, that UCF shares data with.

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

RELATED DOCUMENTS:

1. 4-008.1 *Data Classification and Protection* policy
    a. https://policies.ucf.edu/

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu

Revision Date	Summary of Change
August 8th, 2019	First Version

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL
(For use by the Information Security Office)

Standards Number: *120*

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv Digitally signed by chrisv Date: 2019.11.12 10:56:24 -05'00' 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