Form No.: OGC-S-2016-03

Information Security Hosted Services Contract Checklist

This assessment of information security items is to be completed for contracts that include hosting of university information on non-UHS servers. This sheet should be submitted along with the proposed contract to UHS Information Security at the campus address - security@* (*uh.edu, uhcl.edu, uhd.edu, uhv.edu). After assessment by UHS information Security, this completed checklist will be returned to the requesting department to be included in the packet submitted to the Office of Contracts Administration (OCA).

General Contract Information - to be completed by requesting department

Department: _____

Contact Person: _____ Title: _____

Campus Mail Code: _____ Telephone: _____ Email: _____

Business Administrator: _____ Title: _____

Campus Mail Code: _____ Telephone: _____ Email: _____

Summary of Contract Terms

Contract with: _____

Federal Tax ID: _____ Contractor Contact Person: _____

Contractor Address: _____

Contractor Phone: _____ Contractor Email: _____

Contract Description: _____

Provide a clear synopsis of the goods/services/events/etc. that will result by entering into this agreement

Brief description of the UHS information to be stored at the hosted services site * Required*:

_____

Contract Term: Start _____ End _____

Total Amount of Contract: $ _____

Does the UHS data to be hosted include Level 1 data as defined in SAM 07.A.08?

Yes ☐ No ☐ Comments: _____

Does the UHS data to be hosted include information specific to individual persons?

Yes ☐ No ☐ Comments: _____

Texas state law requires cloud computing services used by state agencies are certified based on criteria provided by the TX-RAMP program (note, the definitions in SAM 07.A.08 differ from the definitions in TX-RAMP). The requesting department should check with the vendor regarding the certification criteria listed below.

The cloud computing service listed above has the following certifications, as defined by TX-RAMP, StateRAMP or FedRAMP (Select all that apply):

☐ TX-RAMP: Identify status: Level 1 ☐ Level 2 ☐ Provisional ☐

☐ StateRAMP: Identify status: Ready ☐ Provisional ☐ Authorized ☐

☐ FedRAMP: Identify status: Ready ☐ Provisional ☐ Authorized ☐

☐ The cloud computing service listed above does **not** require certifications according to TX-RAMP.

Assessment of Information Security Items – to be completed by UHS Information Security

Ownership of UHS Data – University of Houston retains ownership of all data and associated intellectual property.

Yes ☐ No ☐ Comments: _____

Access to UHS Data –Will anyone outside of hosted service employees have access to UHS data?

Yes ☐ No ☐ If yes, who? _____

Will UHS be informed of any changes of access to UHS data related to the previous question?
Yes ☐ No ☐ Comments:_____

Information Security Program for Infrastructure Hosting UHS Data – The hosted service is responsible for having implemented a security program that includes operating system updates and patches, vulnerability testing and other controls providing protections and safeguards for the infrastructure where UHS data resides.

Does the contract contain information about their security program?
Yes ☐ No ☐ Comments:_____

What, if any, audits/certifications are held (SOC1/SAS70, ISO 27001, etc.) and the schedule for reviews?
List:_____

Service Continuity and Disposition of UHS Data – Upon termination of the contract for services, is all UHS data made accessible to UHS staff for export/download to meet record retention requirements?
Yes ☐ No ☐ Comments:_____

Is there a provision that all backups and any other instances of UHS data maintained by the hosted service are securely destroyed and notices of removal provided to UHS?
Yes ☐ No ☐ Comments:_____

Are business continuity and disaster recovery provisions defined as they relate to services provided to UHS?
Yes ☐ No ☐ Comments:_____

Security Incidents and Data Breaches – In the event of any security incident involving a potential breach or disclosure of UHS data, the hosted service must provide timely notification of the incident to UHS. This notification should provide basic information about the incident, as well as corrective actions taken.

Is notification provided to UHS in the event of a potential breach or disclosure of UHS data?
Yes ☐ No ☐ Comments:_____

Upon request, are UHS staff provided access to log information related to investigations involving UHS data/users?
Yes ☐ No ☐ Comments:_____

Are provisions included regarding indemnification and defining responsibilities for notification of affected UHS users?
Yes ☐ No ☐ Comments:_____

Legal Requests for Access to UHS data – Is the process noted as to how the hosted service will respond if provided with a legal request (subpoena, etc.) for access to UHS data?
Yes ☐ No ☐ Comments:_____

Unless restricted by stipulations in the legal request, does UHS receive notification in advance of UHS data being provided?
Yes ☐ No ☐ Comments:_____

Compliance with Information Protection Requirements – Does the contract specify compliance with FERPA?
Yes ☐ No ☐ Other compliance requirements - PCI, HIPAA, etc.? List:_____

Compliance with the European Union's General Data Protection Regulation (GDPR)? – Does the contract specify compliance with the GDPR?
Yes ☐ No ☐

Date received by UHS Information Security:_____

Completed by: _____ _____
Signature Date

Approved by: _____ _____
Signature Date