THE UNIVERSITY OF ARIZONA
Compliance Office

Information Security & Privacy Addendum: Article Assignments

Purpose: Risk owners across the University must decide what level of risk they are willing to accept, and how they will ensure compliance with University policies. This document is designed to provide guidance so that those who are the final decision makers can make a risk informed decision.

1. **Definitions (Article 1):** Updated definitions to reflect 2021 statutory and case law landscape.

Definition	**Assignment**
Cloud Software	UITS and Clark Hill[1]
European Economic Area (EEA)	Privacy
Medical Records	HIPPA Privacy Office
Network	UITS and Clark Hill[1]
Process or Processing	Privacy
Personal Information	Privacy
Security Incident	ISO/Privacy
System	UITS and Clark Hill[1]
University Data	Privacy

2. **Restrictions on University Data Use:** Clarifies when and what happens to University Data during and at the end of the relationship with the vendor.
Article Assignment: Privacy

3. **Written Information Security Program (WISP):** A document that details a vendor's security controls, processes, and policies. A WISP is not a policy, it outlines a vendor's processes and procedures to protect the privacy of personally identifiable information. It's required by multiple state statutes and will likely be required by others (or referenced in a federal law) in the future.
Article Assignment: ISO – can advise whether a particular WISP meets UA policy requirements; Privacy – privacy related questions

4. **Data Privacy & Security:** Outlines vendor requirements to implement and maintain security controls in accordance with industry best practices at a level sufficient to secure University Data.
Article Assignment: Privacy

5. **Representations & Warranties**: New and prudent

Regulation	**Assignment**
GDPR	Privacy
FERPA	Registrar [Alex Underwood] or Privacy
HIPAA/HITECH	HIPAA Privacy Office
GLBA	Bursar's Office or FSO
COPPA	Office of Youth Safety [Jocelyn Gehring]
PCI	Bursar's Office [Robbyn Lennon]

February 2021

6. **Data Security Incident**: Provides information UA will need, including timeline and detail of notice, to fulfill our statutory responsibilities, such as a root cause analysis, a list of those impacted, responsive actions taken, etc.
   Article Assignment: Privacy partners – HIPAA; PCI; FERPA; Personally Identifiable Information

7. **Audit & Testing**: Addresses the requirement to complete: (1) an audit at least annually and immediately after any actual or reasonably suspected Security Incident (and which audits UA will accept), (2) penetration testing, and (3) vulnerability scans.
   Article Assignment: ISO – can advise on areas covered by UA ISO policies and best practices

8. **International Transfers**: Adds GDPR language and the requirement that if UA provides written consent to transfer Personal Information from EEA countries to countries outside the EEA, the terms set out in the EU Standard Contractual Clauses will apply.
   Article Assignment: Privacy

9. **Insurance**: Adds Cybersecurity insurance requirements which incorporates industry-standard reasonable ask with minimums that reflect typical current costs associated with breaches.
   Article Assignment: Risk Management

10. **Appendices**

    a. **Cloud Software**: Additional requirements if the Services provided are provided to UA as Cloud Software.
    Article Assignment: UITS or Clark Hill[1]

    b. **PCI**: Additional requirements if the Services provided involve processing credit and/or debit card transactions.
    Article Assignment: Bursar's Office [Robbyn Lennon]

    c. **PHI: Business Associate Agreement**: Updated to reflect current regulations.
    Article Assignment: HIPAA Privacy Office

[1] Privacy Office can determine when escalating a concern to Clark Hill is appropriate and the process to do so.

Consultation and Escalation Requests

Consultation

1. Requesting a consultation
   a. Enterprise systems/solutions (Google, Zoom, DocuSign, etc.)
   b. On-line proctoring agreements
   c. Novel solutions that involve data collection/processing (facial recognition technology)
   d. When the Addendum doesn't cover the type of contract you are reviewing
   e. Addendum will cover most of the University's agreements, but not all of them.

Escalation

1. When to Escalate
   a. Rejected red lines and you need help responding
   b. Audits: doesn't have one, old audit, bad audit, won't produce one
   c. Doesn't have policies or won't provide them to you (ex: Privacy, Data Processing, etc.)
   d. Vendor cannot commit to only hosting and accessing University Data in the U.S.
      i. In this case, ask for a list of countries
      ii. If vendor can't produce, this is a red flag
2. Who do you contact?
   a. Use this document for guidance on who to contact
   b. Some lanes will only have 1 office, some will have cross-over (ex: ISO – technical expertise & Privacy – interpretation of regulations)
   c. If you don't know, email the Privacy Office

Tips

1. Reach out at the beginning of the contracting process
2. Won't always be clear, use your intuition
3. Be mindful of timeframes when asking for a consult. For lengthy agreements, it will take time to review.
4. Privacy: Complete the 3rd Party Security & Privacy Review Questionnaire and send to the Privacy Office
5. ISO: Complete a Consult Request
6. Email addresses for other Compliance/Privacy Partners

   Risk Management
   Export Control
   PCI
   HIPAA