THE OHIO STATE UNIVERSITY

UNIVERSITY LIBRARIES

3rd Party System Assessment & Service Owner Responsibilities

Scope: The scope of this document is two-fold. First, it is intended to offer guidance on the data retention (and disposition) aspects of Ohio State University **3rd Party Security Risk Assessments**. This guidance should be used both in conducting the assessments as well as during the Assessment Working Group (AWG) and Security and Trust Advisory Board (STAB) evaluation of the assessments. Capturing additional information during the assessment will be beneficial in more accurately determining:

- Compliance capabilities of the application
- Risk scoring
- Positive and negative aspects of the system

Second, this document addresses the on-going records management aspects that **service owners** should keep in mind once the system is in use and throughout the lifecycle of the records and the system, which are often different.

Security Risk Assessment

Sponsor information that should be known going into, and recorded on, the assessment should include:

- Ohio State retention schedule, record series, and retention period that the data proposed to be created by or stored in the system fall under.
  - Record series can be difficult to determine based solely on the data elements. It is helpful to understand how the elements are put together to form records and the purpose/function/use of the application.
  - There could be more than one record series, with differing retention periods, in an application.

Identifying the above pieces of information will help to ensure that the retention period is the *official university approved retention*. If no retention schedule and record series exist, Records Management will need to create it in order to stay in compliance with state law. University Records Management can assist, along with the business unit, in determining this information.

Vendor response to the question "Do you purge application data according to a defined data retention schedule?" should include the following details:

- What is the data purge cycle?
- Does the application have capabilities to automatically purge data at the end of Ohio State approved retention periods? If no, are there manual purge capabilities?
- Can different records (groups of data) be purged on differing cycles?
- Are backups purged on a regular basis? How long are backups retained after the data is purged?
- If the vendor intends to retain data beyond OSU retention or beyond the end of the contract, is the data de-identified?

Precise retention/disposition information from the university and the vendor will allow the governance groups to ascertain whether the difference in risk is acceptable or will require mitigation *prior* to purchase and implementation.

Additionally, having more precise information on the Ohio State retention schedule and record series, along with the vendor purge cycles clearly identified can serve toward proof of legal disposition.

Additional considerations when completing Assessments:

- The existence of a data retention policy from the vendor does not automatically mean it should be considered a positive during the assessment. Whether it is considered positive or negative is dependent upon the contents of the data retention (and disposition) policy itself; its ability to comply with Ohio State retention schedules; whether the vendor retains the information longer than Ohio State schedules require; or whether the vendor does not retain the data long enough per Ohio State schedules.
  - These assessments, at least portions of them, are public record. When a bad data retention policy is listed as a positive, it could be viewed as an endorsement of the vendor's policy.
- If possible during the assessment collect a copy of the vendor's retention and disposition policy and procedures.

Service Owner Responsibilities

- Consider including actionable vendor follow-ups, such as the implementation of retention and disposition, in the Risk Assessment Management Platform (RAMP) or another internal tracking system, for audit and compliance purposes.
  - Periodically check to ensure that the vendor is following the retention and disposition policy. *Having a retention policy only mitigates security issues if disposition of records past their retention actually occurs.*
  - Disposition of Ohio State's records must to be documented, per 2A of OSU's Records Management policy and ISCR DAT3 D. This can be done manually by completing the Certificate of Records Destruction or work with Records Management to determine if system disposition logs or reports will be sufficient.
- End of contract
  - If the vendor's data retention policy is to retain all data until the contract ends, they could be retaining Ohio State data unnecessarily long, which can be a liability.
  - Data that has not yet met retention will need to be exported and retained, in a readable format, beyond the end of the contract in accordance with Ohio State retention schedules.
- Consult with University Records Management

Applications create and maintain records. Not only can Records Management help with the assessment process, but Records Management should be aware of the types of records being created and maintained in order to ensure that the university is compliant of other areas of state and federal law in addition to security and privacy.

For more information or for assistance on records retention schedules and disposition processes, contact:

Pari Swift	**Beth Crowner**
University Records Manager	*Records Management Coordinator*
Swift.102@osu.edu	Crowner.7@osu.edu
614-292-4092	614-688-2934

Additional records management resources can be found at https://library.osu.edu/osu-records-management.

Learn more about Information Security Working Groups, including the Assessment Working Group, at https://cybersecurity.osu.edu/cybersecurity-ohio-state/information-security-groups/security-advisory-board/assessment-working.