UAB TECHNOLOGY PURCHASE GUIDE

When you’re looking to purchase a new technology solution or system, we need your help before we can review the tool.

Ask yourself:

Is this technology going to store, come into contact with, or send any kind of data to another system/solution?

If the answer is yes, follow the steps in this guide.

Step 1 Determine the data classification

IF THIS SYSTEM/SOLUTION IS BEING USED FOR RESEARCH:

Has the data classification been assigned by the sponsor?

Provide data classification.

DETERMINING THE DATA CLASSIFICATION

PUBLIC DATA

Data that may be disclosed to the general public without harm.

EXAMPLES: public phone directory, course catalogs, public research findings, enrollment figures, public web sites, general benefits data, press releases, newsletters, etc.

SENSITIVE DATA

Data that should be kept confidential. Access to these data shall require authorization and legitimate need-to-know. Privacy may be required by law or contract.

EXAMPLES: FERPA, budgetary plans, proprietary business plans, patent pending information and data protected by law.

RESTRICTED/PHI DATA

Sensitive Data that is highly confidential in nature, carries significant risk from unauthorized access, or uninterrupted accessibility is critical to UAB operation. Privacy and Security controls are typically required by law or contract.

EXAMPLES: HIPAA PHI, Social Security numbers, credit card numbers (PCI DSS), GLBA data, Export Controlled data, FISMA regulated data, log-in credentials, and information protected by non-disclosure agreements.

NOTE REGARDING RESEARCH DATA CLASSIFICATION:

The classification of research data depends on several factors that can and often do change as research progresses. It is incumbent upon the researcher to know the type of data and the circumstances governing the data, and classify it accordingly.

If you are not sure of the data classification, please contact your technology liaison and/or your department’s Information Security Liaison to assist you. If you are still unable to determine the classification, please provide the following and email DSO-RiskMgt@uab.edu.

» Description of how you will be using this solution/system

» List all data fields you’ll be collecting (if non-HIPAA data, include sample data set)

Once you have the data classification, please go to Step 2.
Step 2: Determine if you need UAB IT’s help

Includes discussing with vendor how they send out emails and single sign on configuration

Public Data
NO UAB IT help needed

For public data not requiring any technical help from UAB IT (including login/SSO, emailing to or from @uab.edu individuals, UAB data, connecting to another system, server, etc), tell us the following:

IF THIS SYSTEM/SOLUTION IS BEING USED FOR RESEARCH:

Has the data classification been assigned by the sponsor?
Provide data classification

How is this solution helping you?

Will this solution be sending out emails?

If you do not want UAB IT’s help, it is your responsibility to talk with the vendor about how to make sure emails are not quarantined. If you want UAB IT’s help, then IT Governance will schedule a vendor phone call to work through this issue. We consider scheduling a vendor phone call part of IT work (see below).

Please give us a couple of key words describing this system/solution.

Attach all documents, including data classification, to the request and submit ticket in the Tech Help portal.

Add the name(s) of anyone in UAB IT that you are currently working with on this request.

EMAIL PROCESS

UAB IT does not perform whitelisting for services which send out email messages. UAB’s AVP-Chief Technology Officer (CTO) and AVP-Chief Information Security Officer (CISO) encourage those services which send out email messages to conform to the technical solutions used to authenticate email messages as legitimate, known as SPF and DKIM. They also recommend that campus communicators take special care in ensuring that any messages are reviewed to ensure that they do not look like spam and/or a phishing scam to recipients. Should Microsoft’s Office 365 email solution mishandle email messages sent to UAB address holders, please feel free to provide samples to UAB IT.
For public data requiring technical help (including login/SSO, emailing to or from @uab.edu individuals, UAB data, connecting to another system, server, etc.), provide the following documentation from you and the vendor:

**IF THIS SYSTEM/SOLUTION IS BEING USED FOR RESEARCH:**

- Has the data classification been assigned by the sponsor?
  
  Provide data classification.

- How is this solution helping you?

- Will this solution be sending out emails?
  
  (See below)

- Please give us a couple of key words describing this system/solution.

- Attach all documents, including data classification, to the request and submit ticket in the Tech Help portal.

- Add the name(s) of anyone in UAB IT that you are currently working with on this request.

**EMAIL PROCESS**

UAB IT does not perform whitelisting for services which send out email messages. UAB’s AVP-Chief Technology Officer (CTO) and AVP-Chief Information Security Officer (CISO) encourage those services which send out email messages to conform to the technical solutions used to authenticate email messages as legitimate, known as SPF and DKIM. They also recommend that campus communicators take special care in ensuring that any messages are reviewed to ensure that they do not look like spam and/or a phishing scam to recipients. Should Microsoft’s Office 365 email solution mishandle email messages sent to UAB address holders, please feel free to provide samples to UAB IT. Our staff can work with the service owner to make adjustments to the content or point out errors with their SPF/DKIM configurations.
How is this solution helping you?

Will this solution be sending out emails?

If you do not want IT’s help, it is your responsibility to talk with the vendor about how to make sure emails are not quarantined. If you want IT’s help, then Governance will schedule a vendor phone call to work through this issue. We consider scheduling a vendor phone call part of IT work (see below).

What areas do you anticipate needing technical help with to implement this system/solution?

Single Sign On (SSO), installation of solution, data file/data connection, maintaining this solution, etc.

Send the vendor this Data Security Risk Assessment and return completed form to us.

Approval from your department’s Technology liaison and/or business unit’s Information Security Liaison for purchase (provide copy of email)

Request approval for using the data from the data steward (provide copy of email)

» HR data: contact Rahul Thadani at rthadani@uab.edu.
» PCI: contact Financial Affairs
» FERPA (student): contact Cynthia Terry at cterry@uab.edu.
» HIPAA: Requires a data security risk assessment from the vendor. Email riskassessments@uabmc.edu.

Please give us a couple of key words describing this system/solution.

Attach all documents, including data classification, to the request and submit ticket in the Tech Help portal.

Add the name(s) of anyone in UAB IT that you are currently working with on this request.

EMAIL PROCESS

UAB IT does not perform whitelisting for services which send out email messages. UAB’s AVP-Chief Technology Officer (CTO) and AVP-Chief Information Security Officer (CISO) encourage those services which send out email messages to conform to the technical solutions used to authenticate email messages as legitimate, known as SPF and DKIM. They also recommend that campus communicators take special care in ensuring that any messages are reviewed to ensure that they do not look like spam and/or a phishing scam to recipients. Should Microsoft’s Office 365 email solution mishandle email messages sent to UAB address holders, please feel free to provide samples to UAB IT.
For sensitive and restricted data, you will need the following before we review:

**IF THIS SYSTEM/SOLUTION IS BEING USED FOR RESEARCH:**

1. **Has the data classification been assigned by the sponsor?**
   Provide data classification.

2. **How is this solution helping you?**

3. **Will this solution be sending out emails?**
   *(See below)*

4. **What areas do you anticipate needing technical help with to implement this system/solution?**
   Single Sign On (SSO), installation of solution, data file/data connection, etc.

   - Send the vendor this Data Security Risk Assessment and return completed form to us.
   - Approval from your department's technology liaison and/or business unit's Information Security Liaison for purchase *(provide copy of email)*
   - Request approval for using the data from the data steward *(provide copy of email)*
     - **HR data:** contact Rahul Thadani at rthadani@uab.edu.
     - **PCI:** contact Financial Affairs
     - **FERPA (student):** contact Cynthia Terry at cterry@uab.edu.
     - **HIPAA:** Requires a data security risk assessment from the vendor. Email riskassessments@uabmc.edu.

   - Please give us a couple of key words describing this system/solution.

   - Attach all documents, including data classification, to the request and submit ticket in the Tech Help portal.

   - Add the name(s) of anyone in UAB IT that you are currently working with on this request.

---

**EMAIL PROCESS**

UAB IT does not perform whitelisting for services which send out email messages. UAB's AVP-Chief Technology Officer (CTO) and AVP-Chief Information Security Officer (CISO) encourage those services which send out email messages to conform to the technical solutions used to authenticate email messages as legitimate, known as SPF and DKIM. They also recommend that campus communicators take special care in ensuring that any messages are reviewed to ensure that they do not look like spam and/or a phishing scam to recipients. Should Microsoft's Office 365 email solution mishandle email messages sent to UAB address holders, please feel free to provide samples to UAB IT. Our staff can work with the service owner to make adjustments to the content or point out errors with their SPF/DKIM configurations.
We must have ALL the documentation before we can start the review process.

FOR MORE INFORMATION ABOUT WHY WE ARE ASKING ABOUT DATA CLASSIFICATION, PLEASE VISIT THESE DATA SECURITY WEBPAGES:

- Data Protection and Security Policy
- Data Protection Rule
- FERPA