IT Council Committee
Meeting Minutes

Date: Wednesday, January 25, 2017
Time: 8:00 AM - 9:30 PM
Location: University Hall, Room 420B (Collaboration Space)


Guests: Christine Ackerman, May Chang (For Dean Wang)

Apologies: Joni Torsella, Robert Ambach, Daniel Ashwood, Mitchell Phelps

1. Review and Approve Minutes (attached - Nelson Vincent)
   • Jeremy Martin motioned to approve; Anton Harfmann seconded the motion. The minutes were unanimously approved.

2. Two Factor Authentication (2FA) (Bo Vykhovanyuk and Nelson Vincent)
   • OIS purchased an enhanced security tool, Duo, to implement 2FA authentication.
   • When logging in to UCFlex portal, a popup will appear that sends a code to a mobile device. The process is very similar to 2FA being used by the banking industry.
   • 2FA can be set to geolocation so if a user logs in from campus once, 2FA will not be required again.
   • Business Core Systems will pilot 2FA later in 2017 and then implementation will be phased in for the rest of UC.
   • UCIT Helpdesk will be trained to support users once it is implemented.

3. Data Governance Committee (Nelson Vincent and Eileen Strempel)
   • Nelson Vincent, Eileen Strempel, and Susana Luzuriaga, Director of Institutional Research, started their roadshow tours yesterday to kick off the Data Governance Committee. Nelson and Susana are co-chairs. They met with deans, assisted deans, and the executive steering committee members.
• Data ownership and validation processes at UC are not always clearly identified or communicated, which poses a risk management issue for compliance.
• The Data Governance Committee will be instituting best practices, creating a data dictionary, data governance policies and develop standardized reports to aid with transparency and consistency.
• The need for data governance was driven in part by new systems being implemented such as Catalyst, Tableau, and to be good data stewards.
• Membership is still being formed. Send suggestions for membership to Nelson or Susana.

4. Updated IT@UC Governance Bylaws (attached – Nelson Vincent & Annette Marksberry)
• Updated bylaws drafted by the ITCAC committee have been shared with all of the IT@UC topical committees.
• The updated bylaws introduce a new initiative intake form to help track issues going through the governance and integrated decision-making processes. The intake form lives in TeamDynamix (TD) and will be made available to all colleges and administrative units to submit ideas, including new strategic initiatives, into the governance structure.
• TD is service management suite of tools in use by the UCIT PMO, and UCIT will soon be rolling it out for incident management at the UCIT Helpdesk. The goal is for UC community members to submit initiatives via TD, for the PMO to perform the initial review, and then route it through the IT@UC governance process. If the request is determined to be an enterprise-wide strategic effort and has funding, it will become a project.
• Electronic voting options have been included in the bylaws to expedite the approval process.
• The bylaws have also helped to share information across all topical committees to standardize membership and committee formation, standardized reporting, etc.
• UC Libraries may use TD to submit a request for an electronic journals repository.
• The process introduced in the bylaws in still being adjusted and will likely evolve as the governance process matures.
• The ITCAC will use a distributed communication plan to introduce the use of the TD as the tool for requesting new strategic initiatives. The plan will be shared across the 5 topical committees, IT Managers, and a presentation to Faculty Senate IT, etc.
• Mat Lab is one software application that could be used to pilot the TD initiative process.
• Anton suggested the electronic voting process be tested next month by approving the bylaws electronically if they are finalized. The committee agreed.
• Contact any of the 5 topical committee co-chairs if you would like to have them present the bylaws at Faculty Senate, or any other committee meeting.
• A governance retreat may take place after the bylaws have been finalized.

5. Policy Updates (Bo Vykhovanyuk)
• Policy Status Matrix (attached)
  i. Policies will be reviewed and updated annually
  ii. The Framework Policy document, which is not exactly a policy but a framework for the process, has helped expedite the policy approval, review, and implementation process.
  iii. Faculty Senate is developing a policy task force to regulate who has access to course material. Bo suggested they refer to the Privileged Access policy, which will be
submitted for approval at the next IT Council meeting. Faculty want to know who has access to their course, why, and what the official policy is.

iv. Sally Moomaw asked for any IT Council members who are knowledgeable of the course access policy and procedure to contact her.

- **Data Governance & Classification Policy (attached)**
  i. It is not a new policy, and has been in effect since 2009. The only changes to policy were to add a classification type for Restricted Data for Export Controls and to allow restricted data to be stored in a restricted folder on Box@UC.
  ii. After some discussion about how the policy would impact the UC community and how the information and requirements would be disseminated, Jane Strasser motioned the committee to endorse the updated policy with some wording changes she suggested; Lorre Ratley seconded the motion. The committee voted unanimously to endorse the updated policy.
  iii. The new Concur Travel system will help with communicating and understanding Export Control issues. Contact Tara Wood for Export Control questions concerning international travel regulations. Export Controls is also covered in the new faculty orientation. More work needs to be done university-wide to improve communication, understanding and implementation for compliance issues relating to Export Control data.
  iv. The updated Data Governance & Classification Policy is posted on the OIS website and referred to on the Export Controls website as well.

- **HIPAA Policy Update**
  i. Overlapping policies were developed by OIS and Office of General Counsel (OGS). Bo motioned the committee to retire the OIS version of the policy and accept the OGS version as the official UC HIPPA policy; Victoria Wangia seconded the motion. The motion was approved unanimously.

- **Adjournment**
  o The committee adjourned at 9:25 AM.
IT Governance By-Laws

1/20/2017

Final DRAFT
IT Governance

The IT@UC Governance Structure consists of the IT Council, IT Council Advisory Committee, and five topical committees — Core Services & Shared Infrastructure, eLearning, Information Security & Compliance, IT Managers and Research & Development.

These committees report to the IT Council, which feeds into the university's Integrated Decision Making process and to the Senior Vice Presidents.

More than 350 students, faculty and staff representatives attend monthly meetings and serve as part of university-wide IT Governance.
IT Council Advisory Committee
Meets monthly, but will address issues as needed. 11 members, including CIO and 10 topical Committee Co-Chairs.

Fire Topical Committees
Meets monthly, members consisting of:
- Students (Undergraduate & Graduate, Faculty, Staff, Departments, Administrative, Alumni, etc.)
- Technical (Campus & Distributed)

User Community
Table of Contents

Cover Page ...................................................................................................................................... 1
IT Governance .................................................................................................................................. 2

1. IT Council ...................................................................................................................................... 5
   i. IT Council Composition ........................................................................................................ 5
   ii. Standard Terms .................................................................................................................... 7
   iii. Voting members ............................................................................................................... 7

2. Governance Process and Workflow .......................................................................................... 7
   i. Meeting Schedule ................................................................................................................ 7
   ii. Initiative Approval Process .................................................................................................. 8
   iii. Open Seat Membership Process .................................................................................... 10
   iv. Electronic Voting Process (See Addendum) ................................................................... 11
   v. Delegate Process/Attendance ........................................................................................... 12
   vi. Communication .............................................................................................................. 12

3. IT Council Advisory Committee ............................................................................................... 12
   i. IT Council Advisory Committee Composition .................................................................... 13
   ii. Voting members ................................................................................................................. 13

4. Topical Committees .................................................................................................................. 13
   i. Committee Charge ............................................................................................................. 13
   ii. Standard Committee Composition .................................................................................... 13
   iii. Standard Terms .................................................................................................................. 14
   iv. Additional Members (Subject Matter Experts) .............................................................. 14
   v. Voting Members ................................................................................................................ 14
   vi. Non-IT@UC Co-chair Election Process ......................................................................... 14
   vii. IT@UC Assistant Vice President (AVP) Co-chair Appointment Process ......................... 14

5. Subcommittee Formation .......................................................................................................... 15
   i. Standard Subcommittee Composition ............................................................................... 15
   ii. Standard Terms ................................................................................................................... 15
   iii. Additional Members .......................................................................................................... 16
1. **IT Council**

The IT Council is the university governance committee chaired by the Chief Information Officer (CIO) and VP for Information Technologies and is advisory to the CIO. This group is charged to:

- Consider all significant IT initiatives, issues and policies that impact the university.
- Work with the CIO to prepare recommendations to the Senior Vice President for Administration and Finance and the Senior Vice President for Academic Affairs and Provost.
- Participate in the university's Integrated Decision Making process.
- Sponsor the creation and maintenance of a university-wide strategic plan for IT at UC that supports academic and research priorities of the university and lives out the objectives of the Blue Ribbon Task Force on Academic Information Technology Report and other related reports and assessments.
- Develop and maintain appropriate IT policies, standards, guidelines, practices and compliance expectations.
- Appoint chairs of, coordinate and oversee the IT at UC Governance Topical Committees—IT Managers, E-Learning, Research & Development, Core Services & Shared Infrastructure, and Information Security & Compliance.
- Create, coordinate, and oversee ad hoc committees as needed.

i. **IT Council Composition**

The IT Council is comprised of the following representatives/designees:
- Vice President for Information Technology and Chief Information Officer
- Senior Vice President for Academic Affairs
- Senior Vice President for Administration and Finance
- Vice President for Health Affairs
- Vice President for Government Relations and University Communications
- Faculty Senate Appointment – Faculty Senate IT Chair
- Faculty Senate Chair
- University Architect and Associate Vice President Planning + Design + Construction
- Vice President for Research
- Council of Deans representative
- Topical Committee Co-chairs
- Undergraduate Student – Student Government President
- Graduate Student – Student Government President
### ii. Standard Terms

<table>
<thead>
<tr>
<th>Position</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President for Information Technology and Chief Information Officer</td>
<td>Permanent</td>
</tr>
<tr>
<td>Senior Vice President for Academic Affairs</td>
<td></td>
</tr>
<tr>
<td>Senior Vice President for Administration and Finance</td>
<td></td>
</tr>
<tr>
<td>Vice President for Health Affairs</td>
<td></td>
</tr>
<tr>
<td>Vice President for Government Relations and University Communications</td>
<td></td>
</tr>
<tr>
<td>University Architect and Associate Vice President Planning + Design + Construction Representative</td>
<td></td>
</tr>
<tr>
<td>Vice President for Research Representative</td>
<td></td>
</tr>
<tr>
<td>Faculty Senate Appointment</td>
<td>One year</td>
</tr>
<tr>
<td>Council of Deans Representative</td>
<td>One year</td>
</tr>
<tr>
<td>IT@UC Associate/Assistant Vice President Planning + committee co-chair</td>
<td>Permanent (6)</td>
</tr>
<tr>
<td>Non-IT@UC committee co-chair</td>
<td>Two-year term (can serve two consecutive terms for a total of four years)</td>
</tr>
<tr>
<td>Students (2)</td>
<td>One year</td>
</tr>
</tbody>
</table>

### iii. Voting members

All members of the IT Council are voting members. Each topical committee will have one vote move forward to IT Council.

### 2. Governance Process and Workflow

The following items apply to all governance groups including: IT Council, IT Council Advisory Committee, topical committees, and subcommittees.

#### i. Meeting Schedule

The IT Council, IT Council Advisory Committee, topical committees, and subcommittees will meet monthly unless otherwise specified.
<table>
<thead>
<tr>
<th>Committee Name</th>
<th>Meeting Frequency</th>
<th>Meeting Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Council</td>
<td>Fourth Wednesday of the month</td>
<td>8:00 am – 9:30 am</td>
</tr>
<tr>
<td>IT Council Advisory Committee (ITCAC)</td>
<td>Third Friday of the month</td>
<td>8:30 am – 10:00 am *</td>
</tr>
<tr>
<td>eLearning Topical Committee</td>
<td>First Wednesday of the month</td>
<td>8:30 am – 9:30 am</td>
</tr>
<tr>
<td>IT Manager Committee</td>
<td>Second Tuesday of the month</td>
<td>9:30 am – 11:00 am</td>
</tr>
<tr>
<td>Research &amp; Development Topical Committee</td>
<td>Second Tuesday of the month</td>
<td>1:00 pm – 2:30 pm</td>
</tr>
<tr>
<td>Core Services &amp; Shared Infrastructure</td>
<td>Second Thursday of the month</td>
<td>10:00 am – 11:30 am</td>
</tr>
<tr>
<td>Information Security &amp; Compliance</td>
<td>Third Thursday of the month</td>
<td>10:00 am – 11:30 am</td>
</tr>
</tbody>
</table>

*ITCAC meeting times are subject to change

ii. Initiative Approval Process

A Strategic Initiative Overview Form should be completed for all new initiatives. The Initiative Overview Form can be completed by a committee, individual, or college/unit. The Initiative Overview Form will be reviewed by the IT Council Advisory Committee to ensure alignment with university strategy and adequate communication to all IT governance committees. IT Council Advisory Committee will provide feedback and recommend next steps. The review process will also validate the creation of a subcommittee or task force before work begins.
Strategic Initiative Request Flow Process

- Request for Change Identified:
  - New, Significant Change to existing, or
  - Retire a Service is submitted through the submission portal.

- Start:
  - Deans of 14 Colleges
  - IT@UC Community
  - Student Services
  - Administration & Finance
  - I.e. Any UC Stakeholder Group

- Submission Portal
  - PMO/SMO: Validation of Submission
    - Completer
      - No
      - Yes
        - IT Governance Co-Chairs
          - Submission Evaluation For Recommendation
            - More Information
              - No
              - Yes
                - Governance Committee(s) Review, Feedback, and Endorsement
                  - Yes
                  - No
                    - IT Council
                      - Recommend
                        - Yes
                        - No

- Pipeline OR Retirement
  - Stop
iii. Open Seat Membership Process

The Open Seat Membership Process provides an inclusive and standardized process for soliciting and identifying new members.

- **Faculty**- Faculty members are nominated by faculty and elected by Faculty Senate. In addition, the Faculty Senate Chair will maintain a list of alternate committee members based on inquiries and interest. The IT Council and its topical committees will draw from this list in the event a replacement or additional faculty member is needed mid-year. The Project Management Office will also be notified by Faculty Senate about election results in April. Co-chairs will in turn contact their newly elected members to welcome and orient them.

- **Staff**- Staff are made aware of committee membership opportunities for the following school year through targeted staff list serves to notify staff about committee membership opportunities. Messaging will request interested parties to contact the Project Management Office by email at ucit-pmo@ucmail.uc.edu. Names and contact information for interested staff will be provided to co-chairs.

- **Students**- Students are encouraged to participate in IT Council and its topical committees. Recruitment of students begins with Student Government. Information about IT council and the topical committees is provided to the newly elected President during April. This information is then disseminated to the student government members during August at the start of the school year. The Student Body President and Vice President are members of IT Council. Additional Student Government members are invited to participate in the topical committees of interest. Student government members who are unable to participate due to schedule conflicts are encouraged to recruit a designee to attend a topical committee. Designees contact the Project Management Office to join a committee. Co-chairs will in turn contact the student who has expressed interest.
### Typical Recruitment Calendar

<table>
<thead>
<tr>
<th>Month</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>No planned recruitment activity.</td>
</tr>
<tr>
<td></td>
<td>No planned recruitment activity.</td>
</tr>
</tbody>
</table>
| February  | 1. Project Management Office provides the Provost Liaison who in turn will provide the Council of Deans the description of IT Council and current topical committees including meeting days and times.  
2. Article sent re: IT Council and current topical committees.  
3. Call for nominations is sent to faculty by Faculty Senate Committee on Committees. |
| March     | 1. Council of Deans includes IT Council as agenda item to encourage participation.  
2. 2nd article sent re: IT Council and current topical committees.  
3. Nominations to committees are due to Faculty Senate  
4. Elections of committee members held by Faculty Senate. |
| April     | 1. Faculty are notified about election results.  
2. Project Management Office is notified about election results. Project Management Office notifies committee co-chairs about their newly elected faculty members.  
3. Co-chairs contact faculty seated on their committees to welcome them.  
| May       | No planned recruitment activity.                                                                                                           |
| June      | No planned recruitment activity.                                                                                                           |
| July      | No planned recruitment activity.                                                                                                           |
| August    | 1. First IT Council and topical committee meetings of the new school year with new members.  
2. Student body president introduces IT Council and topical committee information to student government. Names of interested students from student government are forwarded to the UCIT-PMO by the President. |
| September | No planned recruitment activity.                                                                                                           |
| October   | No planned recruitment activity.                                                                                                           |
| November  | No planned recruitment activity.                                                                                                           |
| December  | No planned recruitment activity.                                                                                                           |

iv. Electronic Voting Process (See Addendum)
To support an efficient and agile governance process, all groups should use the Electronic Voting Process when initiative approval timelines are more aggressive than the meeting schedule.

Initiative Overview Forms that have been reviewed/approved by the ITCAC will be distributed in advance of any requested vote. A one-week review and question period will culminate in a vote. Voting will be open for 24 hours to allow for individuals on IT Council who are traveling etc.

Members may vote yay, nay, additional information or discussion required, or abstain (a non-vote will be considered an abstention).

v. Delegate Process/Attendance

Sending a delegate is encouraged if a member is unable to attend a meeting. Delegates do not vote.

vi. Communication

All documentation requiring a vote will be distributed at least one week in advance of any governance meeting.

<table>
<thead>
<tr>
<th>Forms</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voting Issue-Action Form Due to PMO</td>
<td>Five Business Days Prior to Meeting</td>
</tr>
<tr>
<td>Agenda &amp; Attachments Sent To Committee Members</td>
<td>Two Business Days Prior to Meeting</td>
</tr>
<tr>
<td>Strategic Initiative Request Form Submitted in TeamDynamix</td>
<td>15th of Each Month</td>
</tr>
</tbody>
</table>

3. IT Council Advisory Committee
The IT Council Advisory Committee (ITCAC) is the university governance committee chaired by an elected member of the committee. The ITCAC is advisory to the CIO and IT Council. This group is charged to:

- Review all significant IT initiatives, issues and policies that impact the university to ensure proper vetting prior to submission to IT Council.
- Work with the CIO and topical committee co-chairs to prepare recommendations to IT Council.
- Review all Initiative Overview Forms.
- Oversee the Open Seat Membership Process.
- Work with the CIO to prepare the IT Council Agenda.

i. **IT Council Advisory Committee Composition**

The IT Council Advisory Committee is comprised of the CIO and co-chairs for each topical committee.

ii. **Voting members**

All members of the IT Council Advisory Committee are voting members.

4. **Topical Committees**

i. **Committee Charge**

The formation of a new committee is at the discretion of the CIO. The initial charge will be developed and delivered by the CIO. Any changes to the charge must be submitted to the IT Council for approval. Committees should review their charge at least annually.

ii. **Standard Committee Composition**

- IT@UC co-chair – appointed by CIO
- Non-IT@UC co-chair – elected from within the committee, nominees must have served at least one year
- Faculty – appointed by Faculty Senate
- Faculty – open seat
- IT@UC Subject Matter Expert – appointed by IT@UC co-chair
• IT@UC Subject Matter Expert – appointed by IT@UC co-chair
• Undergraduate Student – appointed by Student Government
• Graduate Student – appointed by Graduate Student Government

### iii. Standard Terms

<table>
<thead>
<tr>
<th>Position</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT@UC co-chair</td>
<td>Permanent</td>
</tr>
<tr>
<td>Non-IT@UC co-chair</td>
<td>Two-year term (can serve two consecutive terms for a total of four years)</td>
</tr>
<tr>
<td>Faculty</td>
<td>Two-years</td>
</tr>
<tr>
<td>IT@UC Subject Matter Expert</td>
<td>Two-years (no term limit)</td>
</tr>
<tr>
<td>Students</td>
<td>One-year</td>
</tr>
<tr>
<td>Additional members identified by co-chairs</td>
<td>Two-years (no term limit)</td>
</tr>
</tbody>
</table>

### iv. Additional Members (Subject Matter Experts)

Committee co-chairs may identify additional members. Any additional members will serve a two-year term and be identified through the Open Seat Membership process.

### v. Voting Members

All members of the standard committee composition are voting members. Co-chairs of committees may identify additional members as voting members.

### vi. Non-IT@UC Co-chair Election Process

Nominations for the Non-IT@UC co-chair should be collected utilizing the Open Seat Membership Process. All nominations must be from existing committee members that have served at least one year. Self-nominations are acceptable. Only designated voting members for the committee are allowed to vote.

### vii. IT@UC Assistant Vice President (AVP) Co-chair Appointment Process

When possible, the IT@UC co-chair should be the AVP most closely responsible for the committee’s area of work. Optionally, the CIO may appoint an IT@UC representative to serve as co-chair.
5. Subcommittee Formation

The co-chairs of a topical committee may form a subcommittee to support the work of the committee. Subcommittees serve as a recommending and advisory body to the governing committee. Subcommittees should be formed only when the work is ongoing. The creation of a subcommittee must be approved through the Strategic Initiative Overview Form process. The initial charge and goals will be developed and delivered by the committee co-chairs. Any changes to the charge and goals must be submitted to the co-chairs for approval. Subcommittees should review their charge and goals at least annually.

i. Standard Subcommittee Composition

- IT@UC Subject Matter Expert co-chair – appointed by IT@UC (AVP) committee co-chair
- Non-IT@UC co-chair – appointed by committee co-chairs
- Faculty – open seat
- Faculty – open seat
- IT@UC Subject Matter Expert – appointed by IT@UC AVP co-chair
- IT@UC Subject Matter Expert – appointed by IT@UC AVP co-chair
- Undergraduate Student – appointed by Student Government
- Graduate Student – appointed by Student Government

ii. Standard Terms

<table>
<thead>
<tr>
<th>Position</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT@UC Subject Matter Expert co-chair</td>
<td>Permanent</td>
</tr>
<tr>
<td>Non-IT@UC co-chair</td>
<td>Two-year term (can serve two consecutive terms for a total of four years)</td>
</tr>
<tr>
<td>Faculty</td>
<td>Two-years</td>
</tr>
<tr>
<td>IT@UC Subject Matter Expert</td>
<td>Two-years (no term limit)</td>
</tr>
<tr>
<td>Students</td>
<td>One-year</td>
</tr>
<tr>
<td>Additional members identified by co-chairs</td>
<td>Two-years (no term limit)</td>
</tr>
</tbody>
</table>
iii. Additional Members

Subcommittee co-chairs may identify additional members. Any additional members will serve a two-year term and be identified through the Open Seat Membership process. This term can be extended to ensure continuity.

iv. Voting Members

All members of the subcommittee standard composition are voting members. Co-chairs of committees may identify additional members as voting members.

6. Task Force Formation

The co-chairs of a committee may form a task force to support the work of the committee. A task force serves as a recommending and advisory body to the governing committee. A task force should be formed only when the work is short-term or project-based. The creation of a task force must be approved through the Initiative Overview Form process. Once approved, a project manager from the IT@UC Project Management Office will be assigned to help create a formal project charter. The project charter must be approved by the committee co-chairs prior to work beginning. The role of the Project Manager ends once the Charter is approved.

i. Standard Task Force Composition

The composition is determined by the need of the task force for the duration of the project.

ii. Standard Terms

All terms are for the duration of the task force.
Addendum - IT Council Electronic Voting Policy

A. Definitions
For the purpose of this policy,
Polling is defined as “The collection of opinions on a subject.”
Voting is defined as “A formal expression of choice regarding approval of a motion or election of an individual.”
“IT Council” is defined as the IT Council itself, the IT Council Advisory Committee and all topical subcommittees.

B. Purpose
The purpose of this policy is to establish guidelines for the use of email polling and electronic voting with regard to the decision-making authority of the IT Council.

C. Scope
This policy will outline the circumstances where email polling and electronic voting are permitted and will detail the guidelines for their use.

D. General
It is the expectation of all committee members that material presented at meetings will be clear, complete and understandable in terms of the requirements placed upon them for action/response. Therefore, the intent of this policy is to ensure that the same comfort level of a regular face-to-face meeting is maintained while providing a clear explanation as to why the mechanism of email polling or electronic voting is being invoked in lieu of a regular meeting.

E. The Policy
Electronic voting is permitted at all IT Council meetings either by
   a. verbal response to the question via live teleconference or videoconference (where anonymity is not required, or where individually recorded votes are not required).
   b. an email sent to the secretary of the meeting (provides a written record of the vote if required or serves as the equivalent of a secret ballot for individuals not actually present in the meeting room).

At the discretion, or with the consent, of the Council or Committee Chair(s), and for matters of an urgent nature, OR time-sensitive matters OR where it would be more expeditious to do so OR when it is not feasible for the committee to meet in person or via teleconference, email polling and/or electronic voting may be used to help facilitate decisions of the IT Council in accordance with the following:
In recognition that decisions are being made using email communication in lieu of a face-to-face meeting, extra effort will be made to ensure that members are provided with sufficient background materials and adequate documentation to support the request for a decision.
All communication will be shared as a group email with all members copied on correspondence including questions, responses and general commentary. All members will select “reply all”
when providing comments so that these will be shared simultaneously with all members and a record will be kept of the email exchange.

If a resolution is required, the Committee Chair may authorize the Secretary to conduct an electronic vote of the members. A clear rationale will be given to the members to explain why a motion is necessary. The question to be answered will be stated clearly in the form of a specific resolution provided for members’ consideration. Respondents will be asked to vote upon the resolution.

In the event of an electronic vote, a reasonable and adequate time will be determined for members to respond to the request for a decision. Members will have the opportunity to declare a conflict and not participate in the vote. Every effort will be made to obtain a response from each member (i.e. allow each person to register their vote). The resolution shall be deemed to have been approved only if, by the end of the time period specified, the Committee Secretary has received approval responses from a majority of the voting members.

Non-response to an electronic vote will be considered an abstention. Voting records will be kept.

A resolution approved by email polling and electronic voting, permitted by the IT Council and passed by a majority of voting members, shall have the same force and effect as a resolution passed at a regularly constituted meeting of the IT Council.

The Council/Committee Secretary shall prepare a summary document noting the purpose of, and any decisions resulting from, the electronic exchange including any subsequent resolutions.

F. Review

This policy will be reviewed at regular intervals, not to exceed three years, to determine whether amendments are necessary.
## OIS Policy Status as of 1/18/2017

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Review Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Information Security</td>
<td>OIS Review in progress</td>
</tr>
<tr>
<td>Data Governance &amp; Classification (formerly: Data Protection)</td>
<td>To be presented to IT Council in Jan 2017</td>
</tr>
<tr>
<td>Information Security Design &amp; Architecture Review</td>
<td>To be presented to IT Council Advisory Committee in Feb 2017</td>
</tr>
<tr>
<td>Privileged Access</td>
<td>To be presented to IT Council Advisory Committee in Feb 2017</td>
</tr>
<tr>
<td>Incident Management and Response</td>
<td>To be presented to Integrated Decision Making</td>
</tr>
<tr>
<td>Acceptable Use of IT Resources</td>
<td>Approved 11/21/2016</td>
</tr>
<tr>
<td>Clean Desk</td>
<td>Approved 7/6/2016</td>
</tr>
<tr>
<td>Data Center Visitor</td>
<td>Approved 7/20/2016</td>
</tr>
<tr>
<td>Electronic Mail</td>
<td>Approved 11/21/2016</td>
</tr>
<tr>
<td>Password</td>
<td>Approved 11/21/2016</td>
</tr>
<tr>
<td>Policy Development Framework</td>
<td>Approved 11/21/2016</td>
</tr>
<tr>
<td>Risk Acceptance</td>
<td>Approved 7/20/2016</td>
</tr>
<tr>
<td>Vulnerable Electronic Systems</td>
<td>Approved 11/21/2016</td>
</tr>
</tbody>
</table>
## Background

The University of Cincinnati (UC) uses a variety of data in support of its teaching, research and outreach missions. Data is a valued resource the university must govern, classify and protect. In addition, federal and state laws require that the university must limit access to certain categories of data to protect the privacy of employees, students, subjects, affiliates and patients.

## Policy

The purpose of this policy and suite of accompanying resources is to help ensure the governance, classification and protection of university data from unauthorized access, damage, alteration or disclosure while preserving the ability of authorized users to access and use institutional data for appropriate university purposes. This policy refers to all university data, electronic as well as paper, (i.e., hard copy). This policy applies regardless of the place of storage and whether used for administration, research, teaching or other purposes.

Data governance is a quality control discipline for assessing, managing, using, improving, monitoring, maintaining and protecting university data. Data governance is used by organizations to exercise control over processes and methods used by their Data Stewards and Data Custodians in order to improve data quality and integrity. When data is created the Data Trustee must classify the data and establish a governance framework for the data that corresponds to the university rules for that data type and applicable federal and state laws.

## Data Classification and Data Types

This policy describes the actions necessary to secure and protect university data defined as Export Controlled data, Restricted data, Controlled data and Public data. See [Data Classification and Data Types](#) for additional information and examples.

- **Export Controlled**: As a means to promote national security, the U.S. Government controls export of sensitive equipment, software and technology. This data is labeled Export Controlled. Trustees, Stewards, Custodians and Users of Export Controlled data must follow all safeguards for Restricted data plus additional safeguards as directed by the Export Controls Office. Trustees, Stewards and Custodians of systems...
that have Export Controlled data are responsible to work with the Export Controls Office to identify appropriate additional safeguards.

- **Restricted**: Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. Users of Restricted data must follow all safeguards for Controlled data plus additional safeguards identified for Restricted data. High levels of security safeguards must be applied to Restricted data.

- **Controlled**: Data is classified as Controlled when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as Export Controlled, Restricted or Public data must be treated as Controlled data. A reasonable level of security safeguards must be applied to controlled data.

- **Public**: Data that is readily available to the public. This data requires no confidentiality or integrity protection. Public data needs no additional protection.

**Minimum Safeguards**

The responsibility of protecting university data is shared by everyone that uses, accesses or stores such data. Required safeguards depend on the data classification. See [Minimum Safeguards](#) for more information.

**Roles and Responsibilities**

There are four data user roles with differing levels of responsibilities. See [Roles and Responsibilities](#) for more information.

- **Trustees**: Senior university officials or their designees who have planning and policy level responsibility for data within their functional areas and management responsibility for defined segments of institutional data.

- **Stewards**: University officials having direct operational-level responsibility for the management of one or more types of institutional data. Data Stewards in coordination with Data Custodians must implement and apply safeguards that meet or exceed the [Minimum Safeguards](#) of each data classification.

- **Custodians**: Central or distributed university units or computer system administrators responsible for the operation and management of systems and servers which collect, manage and provide access to institutional data.

- **Users**: University units or individual university community members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the university.

Collectively these parties are responsible for identifying and implementing safeguards for the different data types. Many university activities involve multiple departments; for such activities that involve access to, or storage of, university data, the procedures and safeguards must be coordinated by all Trustees, Stewards, Custodians and Users involved.
Compliance and Remediation

University community members must report actual or suspected criminal activity to the Department of Public Safety or, if off campus, other appropriate law enforcement agencies. Incidents involving Export Controlled data must be immediately reported to the unit head, the IT@UC Office of Information Security (OIS) via e-mail at abuse@uc.edu and to the Export Controls Office via e-mail at exportco@uc.edu. In addition, any breach, loss, or unauthorized exposure of Restricted or Controlled data shall be immediately reported to the unit head and OIS via e-mail at abuse@uc.edu. OIS will then determine the appropriate actions to comply with university Policy and local, state and federal law. See Compliance and Remediation and the Incident Management and Response Policy for additional information.

Cloud Based File Storage

Export Controlled data is not permitted to be stored or shared via cloud based file storage of any kind. Only university approved cloud based file storage may be used for Restricted and Controlled data. See Cloud Based File Storage for more information.

Contact Information

IT@UC Office of Information Security  513-558-ISEC (4732)  infosec@uc.edu

Related Links

The Data Governance and Classification Policy subparts:

- Data Classification and Data Types
- Minimum Safeguards
- Roles and Responsibilities
- Compliance and Remediation
- Cloud Based File Storage

Export Controls Office

Revision History

Issued: 07/01/2009
Revised: 08/01/2014
Revised: 08/01/2015
Draft: 12/09/2016
Data Governance & Classification Policy 9.1.1.A
Data Classification and Data Types

Draft Date: 12/09/2016
Effective Date: 5/30/2014
Prior Effective Date: 7/1/2009

Data Classification and Data Types

Various data types have different levels of sensitivity and access that is governed by different laws. The four types of classifications defined in this document are: Export Controlled, Restricted, Controlled and Public. The Data Trustee is ultimately responsible for deciding how to classify their data (see Roles and Responsibilities for list of Data Trustees and additional information).

On a periodic basis, it is important to re-evaluate the classification of university data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the university. This evaluation must be conducted by the appropriate Data Trustee. Conducting an evaluation on an annual basis is recommended; however, the Data Trustee must determine the frequency that is most appropriate based on need. If a Data Trustee determines that the classification of a certain data set has changed, an analysis of security controls must be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they must be corrected in a timely manner, commensurate with the level of risk presented by the gaps. If you have any questions related to classification of data, please contact the IT@UC Office of Information Security (OIS) at 513-558-ISEC (4732) or infosec@uc.edu.

Data Types

The University of Cincinnati has defined four Data Types and created a data classification for each university data: Export Controlled, Restricted, Controlled and Public. The following sections will define these data and provide examples of each type:

Export Controlled

As a means to promote national security, the U.S. Government controls export of sensitive equipment, software and technology. This data is labeled Export Controlled. Trustees, Stewards, Custodians and Users of Export Controlled data must follow all safeguards for Restricted data plus additional safeguards as directed by the Export Controls Office. Trustees, Stewards and Custodians of systems that have Export Controlled data are responsible to work with the Export Controls Office to identify appropriate additional safeguards.

The following table contains examples of Export Controlled data. Please note this is a list of common examples and not an exhaustive listing. Please work with the Export Controls Office if you require additional assistance.
Export Controlled

- Any information labelled Export Controlled or ITAR USML Category or EAR CCL ECCN or any DoD Distribution Statement other than A.
- Information or technology subject to the authorization requirements of 10 CFR part 810, or Restricted data as defined in section 11 y. of the Atomic Energy Act of 1954, as amended, or of other information, data, or technology the release of which is controlled under the Atomic Energy Act and regulations therein.
- Proprietary or 3rd Party information not in the public domain or being published, must be protected until an export classification determination is complete.

Restricted

Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. Users of Restricted data must follow all safeguards for Controlled data plus additional safeguards identified for Restricted data. High levels of security safeguards must be applied to Restricted data.

The following table contains examples of Restricted data, please note this is a list of common examples and not an exhaustive listing. Please work with the Data Trustee and OIS if you require additional assistance classifying data.

<table>
<thead>
<tr>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personally Identifiable Information</strong></td>
</tr>
<tr>
<td>Personally Identifiable Information (PII) that consists of an individual’s name, including the last name along with the individual’s first name or first initial, in combination with and linked to any one or more of the following data elements:</td>
</tr>
<tr>
<td>• Social Security number or partial Social Security number</td>
</tr>
<tr>
<td>• Driver’s license number</td>
</tr>
<tr>
<td>• State identification card number</td>
</tr>
<tr>
<td>• Passport number</td>
</tr>
<tr>
<td>• United States Permanent Resident Card or similar identification</td>
</tr>
<tr>
<td>• SSID – Statewide Student Identifier</td>
</tr>
<tr>
<td>• Financial account number</td>
</tr>
<tr>
<td>• Credit card number</td>
</tr>
<tr>
<td>• Debit card number</td>
</tr>
<tr>
<td>• Electronically stored biometric information</td>
</tr>
</tbody>
</table>

**HIPAA**

For more HIPAA information please view the university's [HIPAA Policy](#).

- Patient names
- Street address, city, county, zip code
- Dates (except year) related to an individual e.g. clinical encounters
- E-mail, URLs, & IP addresses
- Social Security numbers or partial Social Security numbers
- Account/Medical record numbers
**Data Governance & Classification Policy v3.5** – Data Classification and Data Types

**Restricted - continued**

- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle id's & serial numbers
- Device id's & serial numbers
- Biometric identifiers
- Full face images associated with HIPAA records
- Payment guarantor's information
- Any PHI not de-identified per the Safe Harbor De-Identification method listed in the university HIPAA Policy

**Employee Information**

- Social Security number or partial Social Security number
- Home address or personal contact information
- Benefits information
- Worker's compensation or disability claims

**Legal Information**

- All data in the Office of the General Counsel unless otherwise classified by the General Counsel

**FERPA Restricted Non-Directory Data**

- Transcripts, defined as any cumulative listing of a student’s grades
- Student financial services information
- Credit card numbers/Bank account numbers/Debit cards numbers
- Birth name is Restricted if a preferred name is selected
- Wire transfer information
- Payment history
- Financial Aid/Grant information
- Student tuition bills

**Donor Information**

- Name
- Credit card numbers/Debit card numbers
- Bank account numbers
- Social Security numbers or partial Social Security numbers
- Amount/what donated
- Telephone/Fax numbers
- Employment information
- Family information(spouse(s)/children/grandchildren)
- Medical history

**Housing Data**

- Name; Credit rating/history
- Financial worth; Income levels and sources, etc.

**Research Information**

- Human subject information
- Lab animal care information
- Proprietary data as classified by an industry sponsor
- UC proprietary or 3rd party information
- Not in the public domain or being information being published
### Restricted - continued

#### Business Information
- Credit card numbers; Bank account information
- Proprietary data covered by confidentiality or non-disclosure agreements such as but not limited to: Contracts or proposals; project specifications; proprietary company data; models, figures, illustrations.
- Purchasing card (P-card) numbers
- Social Security or other taxpayer ID numbers
- Contract information (between UC and third parties)

#### ISO Number
- Bearcat Card
- Campus Recreation Center
- Parking and Housing
- Administration and operation of the Card Access/Badge system including creating ISO number replacement for lost badges
- Contract information (between UC and third parties)
- Remote student printing service
- Swipe UC IDs for Patron record checkouts in the libraries
- Campus dining and meal plans
- UC Bookstore
- Time clock in/out
- GradesFirst
- Tutor Trac
- DAAP System
- eProfessional
- Blackboard
- UCFileSpace
- Data Warehouse
- Identity Management

#### Miscellaneous Restricted Data
- Data that the university classifies or determines to be highly sensitive

### Controlled

Data is classified as Controlled when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as Export Controlled, Restricted or Public data must be treated as Controlled data. A reasonable level of security safeguards must be applied to controlled data.

The following table contains examples of Controlled data, please note this is a list of common examples and not an exhaustive listing. Please work with the Data Trustee and OIS if you require additional assistance classifying data.
## Controlled

### FERPA Controlled Non-Directory Data
- Graded work, grade book, etc.
- Name; Birth name is controlled if no preferred name is selected
- Date of birth
- Place of birth
- Directory address and phone number
- Electronic mail address
- Mailing address
- Campus office address (for graduate students)
- Secondary mailing or permanent address
- Residence assignment and room or apartment number
- Dates of attendance, i.e. specific semesters of registration
- Enrollment status
- UC degree(s) awarded and date(s)
- Major(s), minor(s) and field(s)
- University degree honors
- Institution attended immediately prior to UC
- ID card photographs for university classroom use
- UCID (unique identifier for all students)
- College and class

### FERPA Controlled Directory Data

*Note that the following data may ordinarily be revealed by the university for Directory Information Purposes without student consent unless the student designates otherwise. If the student designates otherwise, then the following data elements must be treated as Controlled data.*

- Name; Birth name is controlled if no preferred name is selected
- Directory address and phone number
- Dates of attendance, i.e. specific quarters or semesters of registration
- Enrollment status, i.e. college, class (frosh, sophomore, etc...)
- UC degree(s) awarded and date(s)
- College and class
- Major(s), minor(s) and field(s) of study
- University degree honors and awards

### Management Data
- Faculty and staff reviews and performance evaluations

### Miscellaneous Controlled Data
- Data from research germane to intellectual property that is not categorized as Restricted
- Data whose integrity must be maintained
- Other data that must be protected but is not classified as Restricted

## Public

Data that is readily available to the public. This data requires no confidentiality or integrity protection.
Related Links

Data Governance & Classification Policy

Contact Information

IT@UC Office of Information Security  513-558-ISEC (4732)  infosec@uc.edu

History

Issued: 7/1/2009
Revised: 5/30/2014
Draft: 12/09/2016
Background

The various units and departments at the university have a multitude of types of documents and data. To the extent particular documents or data types are not explicitly addressed within this document, it is the responsibility of the Data Trustee to classify data by considering the potential for harm to individuals or the university in the event of unintended disclosure, modification or loss. Departments must be particularly mindful to protect sensitive personal information, such as social security numbers, Driver’s license numbers and financial account numbers; the disclosure of which may create risk of identity theft.

Minimum Safeguards by Classification Level

This document describes the actions necessary to secure and protect university-owned data classified as Export Controlled data, Restricted data, Controlled data and Public data.

Export Controlled

As a means to promote national security, the U.S. Government controls export of sensitive equipment, software and technology, this data is labeled Export Controlled. Users of Export Controlled data must follow all the safeguards for Restricted data plus additional safeguards as directed by Export Controls Office. The Data Trustees, Stewards, Custodians and Users of systems that have Export Controlled data are responsible to work with the Export Controls Office to identify appropriate additional safeguards. The Export Controls office must be contacted for information on proper disposal of electronic equipment that contains Export Controlled data.

Restricted

Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. Users of Restricted data must follow all the safeguards for Controlled data plus additional safeguards. High levels of security safeguards must be applied to Restricted data.

Controlled

Data should be classified as Controlled when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as Export Controlled, Restricted, or Public data must be treated as Controlled data. A reasonable level of security safeguards should be applied to Controlled data.
The table on the next 4 pages contain safeguards for Restricted and Controlled data.

<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Controlled</th>
<th>Restricted</th>
<th>General Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Security software must be installed, enabled and kept up to date to protect against malicious applications, viruses, spyware and malware-based attacks.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td><strong>Recommended</strong></td>
<td><strong>Mandatory</strong></td>
<td>Encrypt via full disk encryption, university owned desktop computers.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Encrypt via full disk encryption, university owned laptop computers.</td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Users must have unique and individual user credentials such as a user id and password per the Password Policy.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Desktop and Laptop computers must have a lockout period of 30 minutes or less in place and must be locked when left unattended.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Laptop computers must be secured via cable locks if not stored in a locked office or desk when left unattended.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>A local firewall must be installed and enabled.</td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Servers, data storage devices and other IT equipment must be kept within secure areas with an appropriate level of physical and environmental controls to protect these resources.</td>
</tr>
<tr>
<td><strong>N/A¹</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td>Internal forms must be revised to eliminate unnecessary references to SSN.</td>
</tr>
<tr>
<td><strong>N/A¹</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td>SSNs should not be stored or used whenever possible, UCID’s should be used instead.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Data stored, used or accessed by an external service provider or agent must have contractual agreement to provide appropriate protection to the same standards as applied at the university. The contract must implement the Data Security Rider and undergo a Security Review.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Office doors must be closed and locked when away from your office, or desk/cabinet drawers/doors must be closed and locked when away from your desk.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Data must not be discussed outside of the workplace or with anyone who does not have a specific &quot;need to know&quot;.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>Electronic equipment containing Restricted or Controlled data must be securely sanitized, transferred or disposed of in a secure manner before leaving possession of the responsible university department.</td>
</tr>
<tr>
<td><strong>The Electronic Media Sanitization Standard:</strong></td>
<td></td>
<td></td>
<td>[ <a href="http://www.uc.edu/content/dam/uc/infosec/docs/Standards/Electronic_Media_Sanitization_Standard_9.1.8.pdf">http://www.uc.edu/content/dam/uc/infosec/docs/Standards/Electronic_Media_Sanitization_Standard_9.1.8.pdf</a> ]</td>
</tr>
<tr>
<td><strong>The Asset Disposition Policy 2.1.15 governs the disposition of all university owned assets and is located at:</strong></td>
<td></td>
<td></td>
<td>[ <a href="http://www.uc.edu/af/budgetfinsvcs/asset/resources.html">http://www.uc.edu/af/budgetfinsvcs/asset/resources.html</a> ]</td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>A robust authentication process consistent with the level of risk associated with unauthorized access is required for access to all Restricted and Controlled data.</td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>User access and login information must be maintained. Security logs must be enabled to maintain a complete, tamper-proof audit trail of all processes initiated by the system and should be forwarded to the central log management system.</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td>Mandatory</td>
<td><strong>Mandatory</strong></td>
<td>All portable storage devices must be encrypted (i.e. USB drives, hard drives, CD's, DVD's and other portable media).</td>
</tr>
<tr>
<td>Data Classification</td>
<td>Data Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlled</td>
<td>Restricted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data access will be granted only when specifically authorized and warranted based on job function. The supervisor of the employee is responsible for reviewing access need.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Once data access is approved, Data Stewards are responsible for notification of the following information specific to the data being requested:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Data documentation and usage guidelines.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Data classification including information on associated state and federal regulations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Required minimum safeguards for protected data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data access authorizations must be reviewed on an annual basis by each Data Steward to ensure that access remains appropriate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access must be deactivated after a period of inactivity not to exceed 12 months.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The supervisor of a transferred employee has 48 hours to confirm that access to applications and resources that need to follow an employee remain in place and that access to applications and resources that do not need to follow an employee are removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terminated employees shall lose access as of their termination date.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N/A²</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anyone accessing or having access to Restricted data must have passed a background check as defined by the university prior to authorization of access to Restricted data. This includes all faculty, students, staff, student workers and affiliates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Any non-university employee accessing Restricted or Controlled data must be sponsored by an employee of the university. The approval process for granting such access must follow the policy of the appropriate Data Trustee. Any non-university individuals accessing university data at the University of Cincinnati are required to comply with federal and state laws and university policies and procedures regarding data security. Sponsorship of access must be reviewed and renewed every 6 months. Access approval records must be maintained according to the appropriate Record Retention schedule.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other than email, only university owned devices may access Restricted data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unpublished research information may only be accessible by those with a &quot;need-to-know&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Based File Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users must only use approved cloud based file storage of university data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sharing is permitted only on a &quot;need-to-know&quot; basis and needs to be approved by the appropriate Data Trustees or Data Stewards for any sharing outside of UC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper Documents, Printers &amp; Fax Machines</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;Clean desk practices&quot; must be in place. Paper documents containing Restricted or Controlled data must not be left unattended and must be protected from the view of passers-by or office visitors. It is recommended that confidential documents contain a cover sheet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paper documents must be shredded when discarded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Classification</td>
<td>Paper Documents, Printers &amp; Fax Machines – Continued</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlled</td>
<td>Restricted</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock file cabinets containing Restricted or Controlled data before leaving the office each day. Utilize a controlled key system for the file cabinets keys or appropriately secure the area.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Store paper documents that contain information that is critical to the conduct of university business in secure file cabinets and keep copies in a secure alternate location.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>N/A(^1)</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper copies of all documents with SSN must be stored in locked filing cabinets and must be shredded when discarded.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Printers and fax machines must be located in a low traffic area that is not accessible to those not authorized to receive the information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Immediately retrieve or secure documents containing university data as they are printed on copy machines, fax machines or printers. Use “Secure Print” if available.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A UC fax cover sheet must be used. The cover sheet must contain a confidentiality statement and contact information for the recipient in the event the fax is received in error.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
<td><strong>Mandatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The fax number of the recipient should be confirmed prior to sending a fax by calling the person or office to which the fax will be sent. Programmed fax numbers should be checked regularly for accuracy.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**University Owned Mobile Device**

| Mandatory | Mandatory |
| A minimum four digit PIN, passcode, fingerprint biometric or pattern must be used to access the device. |
| Mandatory | Mandatory |
| An inactivity timeout to automatically lock the device after a maximum of 5 minutes. (A one minute timeout is recommended.) |
| Mandatory | Mandatory |
| Device encryption must be enabled. |
| Mandatory | Mandatory |
| Automatic data wiping after ten failed PIN, passcode, or pattern attempts must be enabled. |
| Mandatory | Mandatory |
| The ability to remotely remove university-owned data from a lost/stolen device upon user or department request or advisement of the Office of General Counsel must exist. |
| Mandatory | Mandatory |
| Unapproved file sharing applications must not be installed or must be disabled. |
| Mandatory | Mandatory |
| Physical control of mobile devices must be maintained. Users and departments must know of location at all times to limit the risk of unauthorized use. |
| Mandatory | Mandatory |
| Users must ensure adequate security and utilize university approved VPN to send or receive university data over public Wi-Fi networks. |
| Mandatory | Mandatory |
| Users and departments must delete all stored university data before reusing, repurposing or discarding the mobile device. See Electronic Media Sanitization Standard for guidance. |

**Non-University Owned Mobile Device Accessing UC Exchange Servers**

| Mandatory | Mandatory |
| It is understood that some users may inadvertently have email that contains Restricted or Controlled data from the UC Exchange email server on a non-university owned device. Before a user can access the UC Exchange email servers with a non-university owned mobile device, the device must meet the following minimum standards: |
| **•** | A minimum four digit PIN, passcode, fingerprint biometric or pattern to access the device |
Non-University Owned Mobile Device Accessing UC Exchange Servers - continued

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>• An inactivity timeout to automatically lock the device after a maximum of 5 minutes. (A one minute timeout is recommended.)</td>
<td></td>
</tr>
<tr>
<td>• Device encryption enabled.</td>
<td></td>
</tr>
<tr>
<td>• Automatic data wiping after ten failed PIN, passcode, or pattern attempts.</td>
<td></td>
</tr>
<tr>
<td>• Enable the ability to remotely remove university-owned data from lost/stolen devices upon user's request or advisement of the Office of General Counsel.</td>
<td></td>
</tr>
</tbody>
</table>

Non-University Owned Computer Accessing UC Exchange Server Email

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Password that complies with university Password Policy</td>
<td></td>
</tr>
<tr>
<td>• An inactivity timeout (screen saver) to automatically lock the device after a maximum of 5 minutes. (A one minute timeout is recommended.)</td>
<td></td>
</tr>
<tr>
<td>• Virus Protection must be installed, up to date and running. Faculty, students and staff of the university can download virus protections at <a href="http://www.uc.edu/infosec/antivirus.html">http://www.uc.edu/infosec/antivirus.html</a></td>
<td></td>
</tr>
<tr>
<td>• Firewall must be enabled</td>
<td></td>
</tr>
</tbody>
</table>

N/A¹ data with social security number is Restricted data, safeguard is not applicable for Controlled data classification.
N/A² Access to Controlled data does not require background check.

**Public**

Public data is information that may be disclosed to any person regardless of their affiliation with the university. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original source documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the university community and no steps need to be taken to prevent its distribution.

**Related Links**

[Data Governance & Classification Policy](#)

**Contact Information**

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu
History

Issued: 7/1/2009
Revised: 5/30/2014
Draft: 12/09/2016
Data Governance & Classification Policy 9.1.1.C - Roles and Responsibilities

Draft Date: 12/09/2016
Effective Date: 5/30/2014
Prior Effective Date: 7/1/2009

Data Trustees

Data Trustees are senior university officials, or their designees, who have planning and policy level responsibility for data within their functional areas and management responsibility for defined segments of institutional data. Data Trustees work with the Chief Information Officer (CIO) to ensure that the appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the entire university.

Data Trustee responsibilities include:

- Assigning and overseeing Data Stewards.
- Overseeing the establishment of data policies in their areas.
- Determining legal and regulatory requirements for data in their areas.
- Promoting appropriate data use and data quality.

Data Stewards

Data Stewards are university officials, or their designees, having direct operational-level responsibility for the management of one or more types of institutional data.

Data Stewards responsibilities include:

- Assisting in developing and maintaining data classification policies.
- Assisting in developing, implementing and managing data access policies.
- Ensuring that data quality and data definition standards are developed and implemented.
- Interpreting and assuring compliance with Federal and State regulations and university policies regarding the release of, responsible use of and access to institutional data.
- Coordinating and resolving stewardship issues and data definitions of data elements that cross multiple functional units.
- Developing, implementing and maintaining a business continuity plan for institutional data under their control. Business continuity is an ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans and ensure the continuity of operations through personnel training, plan testing and maintenance.
- Providing communications and education to Data Users on appropriate use and protection of institutional data.
• Developing, implementing and communicating record retention requirements to the university community in conjunction with University Archives.

Data Steward’s with responsibilities that include Restricted data such as social security numbers, must also work with other Data Stewards and Data Custodians with similar responsibilities to:

• Review and approve Restricted data usage and use requests.
• Ensure that individuals with visibility to social security numbers have completed required training and that agreed to confidentiality statements.
• Perform periodic reviews to ensure continued compliance with the Data Governance and Classification Policy and all other university policies.

Data Custodians

Data Custodians are central or distributed university units or computer system administrators responsible for the operation and management of systems and servers which collect, manage and provide access to institutional data. Data Custodians must be authorized by the appropriate Data Steward.

Data Custodian responsibilities include:

• Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody.
• Complying with applicable university computer security standards.
• Maintaining disaster recovery plans and facilities appropriate to business needs and adequate to maintain or restart operations in the event systems or facilities are impaired, inaccessible, or destroyed.
• Managing Data User access as prescribed and authorized by appropriate Data Stewards.
• Following data handling and protection policies and procedures established by appropriate Data Stewards.
• Complying with all Federal and State regulations and university policies applicable to the institutional data in their custody.

Note: University units that develop databases and/or systems from institutional data sources and then provide access to this data to other users are considered Data Custodians. These Data Custodians must be authorized by the appropriate Data Steward, approved to further redistribute institutional data and must implement the minimum required safeguards for the source data as prescribed by the Data Steward.

Data Users

Data Users are university units or individual university community members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the university. This access is granted solely for the conduct of university business.
The Data User’s responsibilities include:

- Following the policies and procedures established by the appropriate Data Stewards.
- Complying with Federal and State regulations as well as university policies, procedures and standards associated with the institutional data used.
- Using institutional data only as required for the conduct of university business within the scope of employment.
- Implementing safeguards prescribed by appropriate Data Stewards for limited access and Restricted data.
- Ensuring the appropriateness, accuracy and timeliness of institutional data used for conducting university business.
- Reporting any unauthorized access, data misuse, or data quality issues to the IT@UC Office of Information Security and appropriate Data Steward for remediation.

Institutional data covered by this policy include but are not limited to:

<table>
<thead>
<tr>
<th>Institutional Data Segment Type</th>
<th>Data Trustee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alumni Relations and Fund Raising</td>
<td>Vice President for Development and Alumni Relations</td>
</tr>
<tr>
<td>Equipment and Asset Management Endowment</td>
<td>Senior Vice President for Administration and Finance</td>
</tr>
<tr>
<td>Human Resources (Compensation, Benefits, Payroll)</td>
<td>Senior Vice President Administration and Finance, Vice President General Counsel</td>
</tr>
<tr>
<td>Legal Procurement</td>
<td>Vice President for Research</td>
</tr>
<tr>
<td>Research Administration</td>
<td>Vice President for Research</td>
</tr>
<tr>
<td>Counseling</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Disability Services</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Student Records</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Student Admissions</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Student Financial Aid</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Budget and Planning Campus</td>
<td>Senior Vice President for Administration and Finance, Vice President for Finance</td>
</tr>
<tr>
<td>Life</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Construction</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Facilities and Space Management</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Financial (General Ledger, Accounts Payable)</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Student Billing and Accounts Receivable</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Undergraduate and Graduate Student Registration and Graduation Services</td>
<td>Vice President for Student Affairs, Vice President for Equity &amp; Inclusion</td>
</tr>
<tr>
<td>Student Health</td>
<td>Senior Vice President for Health Affairs, Dean of the College of Medicine</td>
</tr>
</tbody>
</table>
### Institutional Data Segment Type | Data Trustee
--- | ---
Tenure | Vice Provost for Academic Personnel
Learning Management Telecommunication and Networking, UCID | Senior Vice President Administration and Finance
| Vice President for Information Technology and Chief Information Officer

**Note:** Instances of some data types, for example sensitive personal items such as social security numbers may be covered by multiple Data Trustees depending on the context of collection and use.

**Related Links**

[Data Governance & Classification Policy](#)

**Phone Contacts**

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

**History**

Issued: 7/1/2009
Revised: 5/30/2014
Draft: 12/09/2016
Data Governance & Classification Policy 9.1.1.D – Compliance and Remediation

Draft Date: 12/09/2016
Effective Date: 5/30/2014
Prior Effective Date: 7/1/2009

Background

University of Cincinnati personnel are responsible for the protection of sensitive data entrusted to our care; therefore, the Data Governance & Classification Policy was created to help provide simplified guidance and direction for compliance in a complex environment.

Compliance and Remediation Requirements

The Data Governance & Classification Policy requires safeguards for Restricted and Controlled data; see the Minimum Safeguards for details. For requirements related to Export Controlled data, please follow all safeguards for Restricted data plus additional safeguards as directed by the Export Controls Office. In support of these requirements, the IT@UC Office of Information Security (OIS) will:

- Provide strategic direction to the university on meeting these requirements.
- Provide education and consulting to the university regarding compliance with this policy.
- Provide remediation training and consulting services to organizations or individuals found to be out of compliance.

The University of Cincinnati reserves the right to suspend access to information systems for suspected violations, pending investigation and resolution. The university reserves the right to terminate access to any user found in violation of its policies, procedures or safeguards.

Breach Notification

In the event of a data breach or a suspected breach certain specific actions must be taken. Refer to the Information Security Incident Management and Response Policy for more complete information. Notification of a breach differs depending on the data type:

- Export Control: Breaches of data in this category must be immediately reported to the unit head, IT@UC Office of Information Security (OIS) and Office of Export Controls.
- Restricted: Any breach of data in this category must be reported to the unit head and OIS.
- Controlled: Breaches of data in this category must be reported to the unit head, who depending on the severity of the breach, may forward the information to OIS.
- Public: No breach notice needed.
Related Links

- Data Governance & Classification Policy
- Information Security Incident Management and Response Policy

Contact Information

IT@UC Office of Information Security  513-558-ISEC (4732)  infosec@uc.edu

History

Issued: 7/1/2009
Revised: 5/30/2014
Draft: 12/09/2016
Background

The University of Cincinnati is committed to maintaining the privacy and security of Export Controlled, Restricted and Controlled data. While fulfilling that responsibility, the university recognizes the need for a cloud based file storage solution that empowers and encourages faculty, staff and students to utilize a secure and reliable collaborative tool that provides anytime, anywhere access to certain university data. As cloud based file storage becomes increasingly prevalent and storage locations proliferate, the advantages of a university approved singular cloud based file storage provider to assist in collaborative academic and research endeavors become evident. The university provides an approved cloud based file storage solution for secure data storage. By providing a secure and accessible data storage solution for faculty, staff and students the university continues to promote and provide for the security of university data while maintaining data accessibility.

Data Classification Restrictions

In order to meet current data security requirements, certain restrictions need to be placed on collecting, processing, storing or sharing certain data within the cloud environment.

All users must use only university approved cloud based file storage options for Restricted and Controlled data. Please refer to Cloud Computing Standard for university approved cloud based file storage options.

Export Controlled data is not permitted to be stored in any cloud storage solution, please contact the Export Controls Office for appropriate university file storage locations.

Restricted and Controlled data is permitted to be stored on Box at UC. Inside each user account for Box at UC, all Restricted data must be stored in the designated Restricted data folder. The Restricted data folder is not permitted to synch to any device. Sharing of Restricted data in Box at UC is on a need to know basis within the university. Any sharing outside the university must be approved by the appropriate Data Trustee or Data Steward.

The university may contract with a third party vendor for a specific cloud based solution. The vendor’s solution must be assessed by IT@UC for compliance with appropriate safeguards and proper alignment with university Information Technology infrastructure.

Data stored on the university approved cloud based file storage is subject to all university eDiscovery policies and procedures.

As a result of the restrictions placed on cloud based file storage, faculty, staff or students will assume responsibility and be held personally liable for any data breach, policy or legal violation
that results from utilizing a cloud based file storage provider not approved by the University.

**Exit Strategy**

Cloud services must not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. The university must determine how data would be recovered from the vendor and/or transferred to a different vendor. The university must also work with the vendor to establish procedures on data sanitization from the vendor’s cloud services.

**Related Links**

[Data Governance & Classification Policy](#)

**Contact Information**

IT@UC Office of Information Security  513-558-ISEC (4732)  infosec@uc.edu

**History**

Issued: 7/1/2009  
Revised: 5/30/2014  
Draft: 12/09/2016