IT@UC
GOVERNANCE

Information Security & Compliance Committee

Meeting Minutes

University Hall, Room 454
December 15, 2016

Present: Mel Sweet, Matthew Clayton, Jane Combs, Megan Pfaltzgraff, Bo Vykhovanyuk, David Baker, Kyle Hern, Lorre Ratley, Tara Wood, Eira Tansey, Jesse Montgomery, Rick Grant, Mark Stockman, Katrina Biscay, Matt Williams, Tina Bosworth, Todd Beekley, Angela Sklenka, Cindy Lusby

Apologies: Conor DuShane, M.B. Reilly

New Business

- **Welcome and Overview**
- **Review of October Meeting Minutes (attached)**
  - Minutes were approved.
- **Two-Factor Authentication (2FA)**
  - 2FA will be implemented early next year for any system that contains restricted data. OIS is meeting with Division of Administration and Finance to determine if a phased implementation approach is best or if 2FA should be implement on all required systems at one time.
  - OIS will perform a security review to determine if Concur, the automated travel and expense system being implemented, will need to use 2FA since it is an externally hosted system.

- **Audit and Risk Subcommittee Meeting Update**
  - This is a subcommittee of the Board of Trustees.
  - Bo and Nelson meet with them annually to provide information security updates, review high-level risks, discuss resources, etc.
  - Bo will share the Risk Assessment Heat Map he presented to the subcommittee with the IS&C committee
  - The Audit and Risk subcommittee members were very interested in information security issues. The Q&A portion of the presentation lasted more than an hour.
  - Some outstanding issues to be addressed are 2FA and mobile device security.
  - Top-level risks specific to IT are:
    - IDM
    - Infrastructure and cohesive security policies

Information Security & Compliance Committee

Committee Co-Chair
Bo Vykhovanyuk
AVP, UCIT
vykhovbn@ucmail.uc.edu
(513) 556-0803

Committee Co-Chair
Lorren Ratley
Dir., Privacy, Office of General Counsel
(513)584-5061

Membership Roster

UNIVERSITY OF Cincinnati

        - Distributed IT structure at UC (results in silos, lack of coordination, duplication of effort, varying security policies, etc.)
        - Data Center

- **Policy Updates**
    - The President's Executive Committee and the Board of Trustees approved five policies (see attached OIS Policy Status Form).
    - The **Information Security Policy and Compliance Framework** guideline (not a policy) was also approved and permits minor changes to be made to the accompanying procedure during the annual review process. Minor changes to the procedure do not have to be approved through the IDM process.
    - Final versions of the approved policies are on SharePoint site and will be distributed to the university community (possibly via TripleD list) early next year.
    - Information Security Review and Privileged Access policies were approved by IS&CC last week after incorporating feedback from the committee.
    - The data from the Restricted Data Inventory Survey sent out in June have been analyzed. (See attached survey questions and heat map results). Survey results have been shared with distributed IT departments and will be used for future in-depth restricted data analysis.

- **Other Security Related Issues**
    - OIS is developing a tool set to help educate users on the rules of appropriate use and storage of restricted data.
    - Katrina Biscay, OIS, tracks university IT security incidents. OIS periodically analyzes the incident data to determine trend lines (are attacks increasing, decreasing, what systems are being attacked, etc.). Recently Katrina started tracking the time from the start of an incident to the time of resolution.
    - Tara Wood, Export Controls, will bring the newly developed Technology Control Plan to IS&CC committee in spring semester 2017 for review and approval. It will need to be submitted through the IDM process for approval.
    - Export Controls may be required to file a report with the UGS when FISMA incidents occur at UC.
    - A subcommittee made up of IS&CC and R&D committee members is forming to develop a UC FISMA policy. UC is required to have a policy in place by December of 2017.

- **Adjourn**
    - Committee adjourned at 11:10 AM.

SharePoint Site for shared documents

University of CINCINNATI	*Policy Title:* **Information Security Review**	*Policy Number:* **9.1.27**
Category: Information Technology	**Effective Date:** Draft as of 12/01/2016	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: IT@UC	**Prior Effective Date:** 2/13/2015	**Responsible Office(s):** IT@UC Office of Information Security

Background

Information security risk assessments (Information Security Reviews) are necessary to identify and document unmitigated risk that may exist on new or existing university information systems or information technology (IT) solutions and provide recommendations to mitigate the identified risk. Information Security Reviews should be performed whenever new IT services or equipment are acquired or when significant changes are made to existing systems, infrastructure or services. An Information Security Review, along with the recommended security controls work to improve the university's security posture.

Policy

Information Security Reviews must be performed in the following scenarios:

- Implementation of new or significant changes to existing university information systems or services that may store or transmit Restricted or Export Controlled data (see the Data Protection Policy 9.1.1 Data Classification and Data Types for additional information)
- Implementation of new or significant changes to existing critical infrastructure (network, firewall, etc…)
- Implementation of new or significant changes to existing enterprise systems
- Implementation of new or significant changes to existing systems that permit 3rd party access to university systems or data.

The IT@UC Office of Information Security (OIS) should perform an Information Security Review in the early stages of a project or purchase, but must be performed prior to implementation. The Information Security Review enforces preventive measures and application of controls to limit the probability of potential threats and vulnerabilities that are likely to occur during the design and architecture phase of a project. It also aligns the security requirements of IT projects, applications, equipment and services ensuring reasonable protection of confidentiality, integrity and availability of university data and systems, while simultaneously enabling the university to attain its mission.

The Information Security Review Form must be completed and submitted to OIS via email at infosec@ucmail.uc.edu for preliminary review and processing per the Information Security Review process.

Once the Information Security Review Form is received OIS team will evaluate and provide required remediation steps (controls) to be completed by the project owners. Following approval, project owners shall be required to supply status updates at progressive stages of project development in alignment with security requirements provided by OIS.

Failure to comply with the security requirements could result in termination of the project or service. Suspended projects or services shall only be recommenced upon compliance with mandated security requirements.

After the Information Security Review has been completed, projects must follow the university Change Management process.

Related Links

Information Security Review Process
Information Security Review Form

Contact Information

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

History

Issued: 11/01/2009
Revised: 05/01/2010
Reviewed: 02/13/2015
Draft: 12/01/2016

University of CINCINNATI	*Policy Title:* **Privileged Access**	*Policy Number:* **9.1.14**
Category: Information Technology	**Effective Date:** Draft as of 11/03/2016	**Policy Owner:** VP & CIO UC Information Technologies
Policy applicable for: Faculty/Staff/Students/ Affiliates	**Prior Effective Date:** 02/15/2015	**Responsible Office(s):** IT@UC Office of Information Security

Background

Due to the operational knowledge and elevated access to sensitive University of Cincinnati (UC) information technology systems, individuals with Privileged or Administrative Access ("Privileged Access") are in a unique position of trust and responsibility. Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data or processes of other users. Proper controls are required to mitigate this increased risk. Privileged Access is typically granted to system administrators, network administrators, and staff performing system/computer account administration or other such employees whose job duties require special privileges over a computing system or network.

Policy

Privileged Access users must use individual accounts with unique user names and passwords that comply with the university Password Policy. If there is a business need for shared credentials, an approved password storage system must be used. Access to the password storage system must be controlled by the university's approved multi-factor authentication.

Three best practices must be utilized for Privileged Access users:

1. The *Principle of Least Privilege* must be followed. Privileged Access users must have access set to the lowest level of access needed to accomplish their job function. Appropriate university leadership must approve all Privileged Access accounts and review all users with Privileged Access annually to determine if Privileged Access is still needed and to review what level of access is appropriate.

2. Privileged Access users should only have access on a *Need to Know* basis. The users should only have access to, and knowledge of, only the data needed to

do their job function.

3. It is a required best practice and the responsibility of each business unit, to utilize a *Separation of Duties* plan whenever possible. Separation of duties is achieved by seperating roles and responsibilities for a high risk business process across multiple people. This reduces risk to systems and university data, especially in case of credential compromise. Regular review of logs is required to monitor Privileged Access users for misuse, and more important if separation of duties is not possible.

Privileged Access users' desktop or laptop computers must be university owned and must be managed by university controlled Endpoint Protection Services. When utilizing Privileged Access to access university systems, users must connect via the university's network. If access is required when off-campus, then user must use the university's VPN and university approved multi-factor authentication. Wherever and whenever possible Privileged Access users must utilize university approved multi-factor authentication.

Individuals with Privileged Access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with all relevant laws, policies and regulation. In all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices and operational guidelines pertaining to the activities of their local department.

Privileged Access use must be reserved for tasks that require the use of Privileged Access. If methods other than using Privileged Access will accomplish a task, those other methods must be used. If a Privileged Access user must submit data or access a system as an end-user, traditional means must be used to submit data or access a system (ie. If a System Administrator must submit their annual benefit elections, they must do so as a normal user and not through Privileged Access not available to other users.) Every user of the system should operate using the least set of privileges necessary to complete the task. This principle limits the damage that can result from an accident or error.

It is important these individuals be familiar with relevant university policies and government regulations. IT@UC personnel with Privileged Access must review the detail of all university policies, specifically those related to information technology. The following polices must be reviewed, understood and implemented:

- Data Protection Policy
- Acceptable Use of Information Technology

- Password Policy
- Other Applicable Information Security Policies

Security training, as directed by the IT@UC Office of Information Security (OIS), must be completed by all Privileged Access users no less than annually or as deemed appropriate by OIS. Data Stewards are responsible for monitoring and records retention for their own faculty, staff and students for compliance with the security training requirement.

Privileged Access users shall take necessary precautions to protect the confidentiality and integrity of information encountered in the performance of their duties. If, during the performance of their duties, users observe strange activity or evidence indicating misuse, they must immediately notify their supervisor and OIS at 558-4732 or abuse@uc.edu. If any criminal activity is suspected, the user must also immediately contact the UC Police Department (UCPD) at 556-1111.

Definitions

Privileged Access*:* Access that allows an individual who can take actions which may affect computing systems, network communication, or the accounts, files, data or processes of other users. Privileged access is typically granted to system administrators, network administrators or other such employees whose job duties require access to sensitive data residing on a system or network. This data can be paper or electronic data. For the purposes of this policy, application and other developers are also considered privileged.

Related links

Data Protection Policy
Acceptable Use of Information Technology
Password Policy
Other Applicable Information Security Policies

Contact information

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

History

Issued: 01/04/2008
Revised: 02/15/2015
Draft: 12/01/2016