UCF | University Compliance, Ethics, and Risk Office

UNIVERSITY OF CENTRAL FLORIDA

University of Central Florida
Draft Policy Submission Cover Memo Form

Policy No. and Title: 4-016.2 Draft Email Policy

Initiating Authority: Vice President for Information Technology and Chief Information Officer

Initiating Authority Approval Date: November 7, 2024

Date of Submission for Review: November 18, 2024

Submitted by: Matthew Fitzgerald

Department: UCF INFOSEC

☐ New Policy ☑ Existing Policy (5-year Review) ☐ Existing Policy Out of Cycle Review

Summary of Revisions: For a new policy, please provide a summary of the policy. For an existing policy, please provide a summary of the revisions made to the policy.

* Updated email provisioning information
* Updated email de-provisioning information
* Removed references to knights email

Stakeholders included in the Review Process: (Provide a list of departments involved in the review/revision process.

Compliance, Ethics, Risk Office
Legal
Research
IT
Faculty Affairs
Audit
College Policy Liaisons
Faculty Senate

Stakeholder feedback must also be requested from the Faculty Senate and the College Policy Liaisons. By checking the boxes below, you are confirming that feedback from these groups was requested, received, and considered in the draft policy.

☒ College Policy Liaisons ☒ Faculty Senate

Regulatory Requirements if applicable)**:** Provide information on regulatory requirements pertaining to the policy, including specific statute or regulation number.

Presenters: (Provide the name s), position title(s), and email address(s for all individuals who will be presenting the policy to the university's Policies and Procedures Committee.

Matthew Fitzgerald, Deputy CISO, Matthew.Fitzgerald@ucf.edu
Lisa Isham, Associate Director, Unified Communications, Lisa.Isham@ucf.edu
Sheila Amin Gutierrez de Pineres, CIO, Sheila@ucf.edu

DRAFT – University Email ~~Provisioning, De-provisioning, and Use~~ Policy

Policy Number 4-016.~~1~~2
Responsible Authority ~~Vice President for Information Technology and~~ Chief Information Officer~~ies & Resources~~
Initiating Authority Vice President for Administrative Operations and Chief Infrastructure~~Information Technology and Chief Information~~ Officer~~ies & Resources~~
Effective Date
Date of Origin 12/13/2017

APPLICABILITY/ACCOUNTABILITY

This policy applies to all persons and entities that are provided an account in the university's electronic mail systems ~~(i.e., Office 365 or Knights Email)~~.

POLICY STATEMENT

Email is a key communication resource provided by the university for the benefit and use of its employees, students, and other authorized user~~other~~s. All email users have the responsibility to use their university-provided email account in an ethical and lawful manner. UCF currently ~~utilizes~~ provides an~~two~~ official enterprise email solution using a industry leading~~s: a~~ cloud-based platform~~system utilizing Microsoft's Office 365 (O365)~~ for faculty, ~~and~~ staff, ~~members for university business use and a separate O365 instance for~~ students, and sponsored guest accounts ~~(Knights Email)~~.

~~A copy of this policy shall be provided to all employees at the beginning of their employment at UCF.~~ Any violation of this policy and procedures may result in the loss of email privileges.

DEFINITIONS

~~**Deleted account**. An email account that has been purged from Office 365. Prior to deletion, contents of an employee account must be copied to a secure location to meet applicable records retention requirements.~~
~~**Disabled account**. Email account status that prevents the user of the account from accessing it. This account status can be changed by UCF IT email administrators or the Information Security Office.~~

Employee. A person who has been officially hired by UCF and has an employee record in the Workday~~PeopleSoft~~ HR system.

Enterprise Resource Planning System (ERP). ~~PeopleSoft~~ Student Information System~~Administration~~, Human Resources (HR), or Financial~~s~~ systems: ERP is the authoritative source of information on Student, HR and Financial~~s~~ data, and identity data on all persons and entities affiliated with UCF.

~~**Expired account**. Email account status that prevents incoming email from being accepted. After six months of expired status the account is deleted. This account status can be changed by UCF IT email administrators or the Information Security Office.~~

~~**Knights Email**. UCF's student email system, supported by a distinct instance of Office 365. Students and current employees may obtain an account at no cost for personal use. Knights Email is the official communication channel for messages from university offices to students.~~

~~**Non-Employee**. A person affiliated with, but not officially employed by UCF.~~

Office 365 (O365). An email service offered by Microsoft Corporation. Office 365 is the email platform supporting UCF's enterprise email service~~ and also Knights Email for students~~.

Phishing. An attempt to acquire sensitive information such as usernames, passwords, and credit card numbers, often for malicious purposes, through electronic communications, such as in email or text messages.

~~**Pre-Employment**. The status of a person who has accepted employment at UCF, and is provisioned in the ERP system, but whose official start date has not occurred.~~

Retiree. An individual who has completed all steps necessary to retire from the university and is officially listed in the ERP system as a Retiree.

Spam. Unsolicited and undesired electronic messages containing advertisements for products or services.

Sponsored Account. A computer or email account created for individuals that do not fit standard employee or student roles, such as consultants, contractors, guests, courtesy appointees, etc.

Student. A person who has been admitted into full-time, part-time, or transient student status and who has a student record in the PeopleSoft student information system. See policy 4-010 Student Email for further details.

University Business. In the context of this policy, electronic mail messages that a person covered by this policy may send or receive in the conduct of their university responsibilities.

GENERAL POLICY

Email Data Ownership

The university owns all university email accounts and content in the *.ucf.edu domain space regardless of the platform or provider ~~(e.g., all Microsoft Office 365) instances~~. ~~The content in the faculty, and staff, and student O365 instance is owned by the university.~~ All u~~U~~niversity business must be conducted by faculty and staff through ~~using~~ provided accounts in the university's enterprise email system and systems authorized to support highly restricted data in accordance with policy~~the~~ 4-217 Controlled Unclassified Information ~~Microsoft Office O365 email system~~~~faculty and staff instance~~.

All~~The~~ university~~O365~~ owned ~~Knights E~~email system~~s~~ ~~is~~are not intended for personal use~~, and therefore the content is personally owned~~. All email content ~~in O365 instances~~ is subject to copyright and other intellectual property rights under applicable laws and university policies.

Email Privacy and Right of University Access

The university will make every attempt to keep email messages secure; however, privacy is not guaranteed, and users should have no general expectation of privacy in email messages sent through university email accounts. Under certain circumstances, it may be necessary for university IT staff or other authorized university officials to access university email accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents or investigating violations of this or other university policies; and, in the case of Microsoft Office 365 Accounts, violations of Microsoft's Acceptable Use Policy or the university's contracts with Microsoft. University IT staff or university officials may also require access to a university email account in order to continue university business where the university email account holder can no longer access the university email account for any reason (such as death, disability, illness, or separation from the university.) Such access will be on an as-needed basis and any email accessed will only be disclosed to individuals who have been properly authorized and have an appropriate need to know or as required by law. The university may access the contents of email accounts for purposes of e-discovery, ~~or~~ officially sanctioned investigations, and/or recovery and preservation of current or former faculty or staff message contents in the event that an employee's work status changes. All email users are bound by the appropriate acceptable use policies of both the university and Microsoft.

Data Retention and Purging

Email messages held in the O365 accounts for faculty and staff are subject to university's storage and email retention policies. O365 mailboxes are set to maximum storage size of one hundred gigabytes and ten years' retention. Any email over the ten-year period will be automatically purged~~,~~ but may be archived by the account holder prior to the end of the ten-year retention period.

Email Record Retention

It is the responsibility of employees to preserve university records, including emails or instant messages in particular circumstances: 1) those who have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed, 2) a subpoena has been served or notice of same has been given, 3) records are sought pursuant to an audit or similar pending or possible investigation, and 4) public records retention as required by Florida statutes or federal agencies.

Appropriate Use and User Responsibility

Highly restricted data, as defined by policy 4-008~~.1~~ Data Classification and Protection, must not be stored or transmitted within the university email system unless the data is encrypted to prevent data loss. Restricted data, as defined by policy 4-008~~.1~~ Data Classification and Protection, may be transmitted or stored within the university email system without data encryption. Sending highly restricted or restricted data from the university email systems to a non-university email system without data encryption is prohibited. Refer to the university's policy 4-008~~.1~~ Data Classification and Protection for further definitions and protections on restricted and highly restricted data.

Please refer to policy 4-006~~.1~~, Broadcast Distribution of Electronic Mail, for the university's requirements on mass email communications.

In order to prevent the unauthorized use of email accounts, the sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with this policy.

All incoming emails are ~~is~~ scanned for malware and spam. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is not possible to guarantee protection against all spam or malware, nor is it possible to prevent blocking of certain legitimate messages. It is therefore incumbent on each individual to take~~use~~ proper care to prevent the spread of malware. In many cases, messages containing or pointing to malware or phishing content appear to be sent from a friend, coworker, or other legitimate sources. Users should not click on links in an email message or open attachments unless the user is certain of the nature of the message and the sender. Suspicious emails should be submitted via the Phish Alert Button or forwarded, as an attachment, to soc~~sirt~~@ucf.edu where they can be investigated.

Personal Email Accounts

To avoid confusing official university business with personal communications, and to adhere to Florida public records laws, employees must not use non-university email accounts (e.g., personal Hotmail, Yahoo, or Gmail accounts) to conduct university business. Forwarding university business related email to a non-university personal email account is not permitted in order to prevent potentially sensitive university information from being sent to external, non-secure email systems.

PROCEDURES

Email Account Creation

Employees and Students

Employees who completed ~~Upon completion of~~ the hiring ~~or pre-employment~~ process within~~, and when an employee record is created in~~ the Human Resources system will be issued a university email address for the purpose of conducting official university business~~, each employee becomes eligible for an email account~~. ~~Creating an email account is initiated through an electronic form by the department's Human Resources Liaison, or delegate, and is based on the employee's role and relationship with the university. Email accounts are created based on the official name of the employee as reflected in the Human Resources system.~~ Students become eligible for an email account through an automated process once fully matriculated for registration; some program matriculation dates may vary.

The standard format for an employee email account is~~:~~ ~~firstname.lastname@ucf.edu~~FirstName.LastName@ucf.edu and for student email, the standard format is NID@ucf.edu. Faculty~~, and~~ staff, and students can establish an alternate, or alias~~, account~~ name by using the self-service process in the UCF IT Support Portal~~myUCF portal~~. Students may only create one email alias.

~~Faculty and staff members can create a Knights Email account in the Knights Email instance for general personal use by using the online form at http://knightsemail.ucf.edu.~~

~~Once student applicants are matriculated, the student becomes eligible for a Knights Email account. Students use the above university-provided provisioning application to create their customized Knights Email account.~~

~~When a student is employed by the university (e.g., part-time employment, GTA, etc.), an email account may be requested by the HR Liaison in the O365 faculty and staff email system for the purposes of conducting university business.~~
UCF issues one email account per individual. If an active employee becomes a UCF student or if a student with an active university email account becomes a UCF employee, the individual will be responsible for setting up a separate folder within their mailbox to store their academic emails to avoid comingling of academic and work-related emails. Upon termination from employment, former employees should anticipate only having access to the content in their academic folder while they remain a current student. All other content may be removed and provided to authorized managers via a request process for the purposes of business continuity.

Hiring managers employing students (e.g., part-time employment, GTA, etc.), who will be expected to use university email as part of their employment are responsible for providing a shared or group mailbox to the student for the purposes of conducting university business. The process for requesting a new or modifying an existing shared or group mailbox is available in the UCF IT Support Portal. In those instances where a shared or group mailbox is not appropriate due to the nature of the student employee's work, managers are required to establish procedures for student employees to maintain separation of their work-related emails from their academic emails, with emphasis on securing highly restricted and restricted data, as defined by policy 4-008 Data Classification and Protection. Once the student discontinues employment with UCF,

managers will not be permitted direct access to the UCF business related email contained in the student's email account and therefore managers must establish procedures for ensuring business continuity. Managers can review knowledge base articles at it.ucf.edu or reach out to UCF IT if they have additional questions.

Sponsored Accounts

Nonemployees who have an active relationship with the university may also be issued email accounts to conduct UCF business at the request of a university employee University employees who sponsor users of guest accounts may request a UCF ~~Sponsored Account and an associated~~ email account for a guest's account. Sponsored account requests for guests are reviewed on a case-by-case basis ~~for~~ and are intended for use by individuals who are not UCF faculty, staff, or students. Sponsored accounts ~~and online resource access~~ can be requested using the https://sponsoredaccounts.infosec.ucf.edu website ~~forms and procedures found on the Service Desk web page at **https://it.ucf.edu**~~. Sponsors are required to request online resource access (e.g., an email account) through the UCF IT Support Portal for sponsored guest accounts. Sponsored accounts are generally established for one year and must be renewed annually. The standard format for a nonemployee email account is: FirstName.LastName@ucf.edu.

Departmental Email Accounts

Requests for shared departmental accounts will be accommodated~~,~~ but require designation of at least one~~an~~ account holder who will administer the addition, deletion, or modification of users within the account, as well as manage the account as per these guidelines. Departmental accounts that have not been signed into for over a year may be deleted.

Granting Access

The university may access the contents of email accounts for purposes of e-discovery, or officially sanctioned investigations at the request of the following university officials or their designee: provost and executive vice president, vice president and general counsel, chief audit executive, or vice president for compliance, ethics, and risk and chief compliance and ethics officer. ~~chief compliance and ethics officer, chief audit executive, or Office of the General Counsel.~~

~~Active Employees and Students~~

~~Request for access to an active employee's email account requires approval from the provost, chief compliance and ethics officer, chief audit executive, or Office of the General Counsel.~~

~~Former Employee~~

~~Request for access to a former employee's email account requires approval from the previous manager and approval from the dean or director of the employee's college or administrative department.~~

Email Account De-Provisioning

Notwithstanding the following procedures, university executives (e.g., president, provost, Office of the General Counsel, etc.) reserve the right to revoke email privileges for cause at any time.

~~**Faculty and Staff who leave before retirement**~~
Staff

Email privileges will be removed for~~Faculty and~~ staff members who are departing and no longer with UCF immediately after ~~leave the university will have email privileges removed effective on~~ their last work~~inged~~ day. If ~~such~~ separation is for cause, email privileges will~~may~~ be immediately revoked without notice. Managers may~~Upon~~ request~~,~~ automatic replies to~~will~~ be added to the email account to notify senders of the former employee's status and/or new contact information. ~~An email account may also be assigned to a manager, or delegate, upon appropriate approvals.~~ In limited circumstances, an email account may also be assigned to a manager, or delegate, upon appropriate approvals. Contents will remain in the account's mailbox as required by current records retention requirements.

Former staff members who are current UCF students will maintain access to their email account. However, upon termination of employment, their non-student, university business-related messages may be removed from their account by or before their last day worked. An out-of-office message can be added to the email account for a selected period of time agreed upon before separation of employment to notify senders of the former employee's status and to direct the sender to an appropriate individual or department email address. The former staff member will be removed from any shared or group mailboxes used by their department, by their manager, by or before their last day worked.

Sponsored Accounts

~~Sponsored accounts must be renewed annually.~~ Sponsored accounts will become disabled if the sponsor of the account does not~~fails to~~ renew the account through the sponsored account process. Once disabled, an email account can be re-activated upon sponsor request.

Faculty who separate from employment before retirement

Faculty members who terminate employment before retirement will have their email privileges removed based on the collective bargaining agreements. If such separation is for cause, email privileges may be immediately revoked without notice. Leadership may request automatic replies to be added to the email account to notify senders of the former employee's status and/or new contact information. In limited circumstances, an email account may also be assigned to a manager, or delegate, upon appropriate approvals. Contents will remain in the account's mailbox as required by current records retention requirements.

Retired Faculty ~~and Staff~~

Faculty ~~and staff members~~ whose positions are or were represented by the United Faculty of Florida (UFF) and have retired from the university will be permitted to retain a university email account as described in UCF Ppolicy 3-001~~.2~~ University Benefits for Retired Employees and the current UCF-UFF Collective Bargaining Agreement.

~~Active Students and~~ Alumni

~~Knights Email accounts are currently not de-provisioned.~~ Students who have graduated from the university or are no longer an active student will be permitted to retain their email privileges for one year after the end of their last UCF registration or graduation (whichever comes first). ~~if the account continues to be actively used. In the event the university terminates or otherwise ceases its contractual relationship with Microsoft regarding the Knights Email system, all accounts will be deleted.~~ Note that some students may retain access longer based on program requirements. Students can ~~Users will be given the option of~~ download~~ing~~ their data at any point prior to account deletion.

Expelled Students

If a student is expelled from the university, email privileges may be terminated immediately at the direction of the Office of Student Rights and Responsibilities.

RELATED INFORMATION

Further information regarding Microsoft's policies on Acceptable Use, Terms of Use, Privacy and Trademarks can be found here:
https://products.office.com/en-US/legal/docid12
UCF Policy 2-100 Florida Public Records Act—Scope and Compliance policy
~~https://policies.ucf.edu/documents/2-100.pdf~~

UCF Policy 2-103~~.2~~ Use of Copyrighted Material policy
~~https://policies.ucf.edu/documents/2-103.pdf~~

UCF Policy 3-206~~.5~~ Credit Cart Merchant Policy

https://policies.ucf.edu/documents/3-206.pdf

UCF Policy 4-007.1 Security of Mobile Computing, Data Storage, and Communication Devices policy
https://policies.ucf.edu/documents/4-007.pdf

UCF Policy 4-001.1 Retention Requirements for Electronic Mail
https://policies.ucf.edu/documents/4-001.pdf

UCF Policy 4-002.2 Use of Information Technologies & Resources Policy
https://policies.ucf.edu/documents/4-002.pdf

UCF Policy 4-006.1 Broadcast Distribution of Electronic Mail
https://policies.ucf.edu/documents/4-006.pdf

UCF Policy 4-010 Student E-Mail
https://policies.ucf.edu/documents/4-010.pdf

UCF Policy 4-209 Export Control Policy

UCF Policy 4-217 Controlled Unclassified Information
https://policies.ucf.edu/documents/4-209.pdf

UCF Policy 4-014 Procurement and Use of Cloud Computing and Data Storage Services
https://policies.ucf.edu/documents/4-014.pdf

CONTACTS

History 4-016 12/13/2017; 4-016.1 10/4/2018