University Standards

UNIVERSITY OF CENTRAL FLORIDA

Subject:	UCF DKIM and SPF Standards
Standards Number:	109
Effective Date:	3/09/2020
Revised Date:	
Responsible Authority:	Information Security Office
Pages:	4

ACCOUNTABILITY/APPLICABILITY:

This standard applies to colleges or departments requesting a vendor managed cloud-based application to send email as @ucf.edu and/or any sub-domain (i.e., spoofed address.)

STANDARDS STATEMENT:

This standard outlines the requirements for authorizing a vendor to send DKIM-authorized mail. It also defines criteria based on business needs for whether the DKIM authorization will be given to the top level @ucf.edu domain versus a unit-level subdomain.

BACKGROUND:

The University of Central Florida has a need to review and authorize vendors that send email as official @ucf.edu correspondence. When a vendor sends an email from a domain that they do not own, that process is known as email "spoofing". Internet Service Providers (ISPs) and spam detection systems are increasingly blocking spoofed emails since spoofing is a well-documented method of email attack. Faculty, staff, students, alumni, university partners, and the general community need to be assured that email with an @ucf.edu sender address is trustworthy and authorized. DKIM (DomainKeys Identified Mail) is recognized as an industry standard for authorizing an outside system to send as another domain. Because each vendor that is authorized to send using DKIM can effectively send as any UCF sender and request personal information, a security review is required. Each vendor must ensure their system provides appropriate controls to prevent unauthorized email sending using the @ucf.edu domain suffix.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

STANDARDS:

1) **Vendor Risk Management** All Vendors that send email using @ucf.edu addresses using DKIM (including subdomains) must go through the Vendor Risk Management process, outlined at https://infosec.ucf.edu/risk-and-compliance/vrm. Departments or Colleges should specify the requirements for using @ucf.edu as the Sender Domain, or an acceptable sub-domain, such as @mail.ucf.edu.

2) **SPF Authorization for @ucf.edu** SPF authorization for @ucf.edu will only be given for vendors with executive level (e.g., CIO, VP, AVP, etc.) approval.

3) **DKIM Authorization for university-level business (@ucf.edu)**
   - Top-level @ucf.edu DKIM authorization is intended for emails generally pertaining to critical university business operations. Only vendor cloud-based applications sending emails for the purposes of supporting critical university business, and after a security review, will be authorized via DKIM for top-level @ucf.edu.
     - Typical examples of DKIM authorized emails include prospective student marketing, admissions correspondence, financial notifications, or official university business correspondence.
   - Vendors should require domain ownership verification for accounts or individuals attempting to send as @ucf.edu. This may include DNS verification TXT record or confirmation email to the UCF account.

4) **DKIM authorization for non-university level business (@[subdomain].ucf.edu)**

   Top-level @ucf.edu DKIM authorization is intended for email activities generally for campus wide, enterprise level business critical functions.. @ucf.edu DKIM Authorization will not be generally given for unit-level systems and for general email marketing campaign purposes. Examples of unit-level or more limited email activities include:
   - Vendors that send email as departments or colleges not directly impacting the university as a whole
   - Vendors sending surveys, questionnaires, targeted marketing, or departmental/college internal newsletters
   - Any vendor that is not sending official university branded correspondence as it relates to university operations

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

Instead, for these unit-level email activities, authorization will be given via one of the following methods:

a) **@mail.ucf.edu** For most unit-level email, DKIM authorization will be given to @mail.ucf.edu
   - Consider using an OID@mail.ucf.edu or first.last@mail.ucf.edu.

b) **Unit-level Subdomains** For units that have their own email subdomain, DKIM authorization will be given to that unit's subdomain (e.g., @fiea.ucf.edu, @bus.ucf.edu, @creol.ucf.edu, etc.)

In either case, vendors should require domain ownership verification for accounts or individuals attempting to send as @[subdomain].ucf.edu. This may include DNS verification TXT record or confirmation email to the UCF account.

5) Emails sent must follow *UCF Mass Email Guidelines*: https://infosec.ucf.edu/awareness/faculty-staff-security-guidelines/mass-email-guidelines/

6) Email addresses used for DKIM-approved mail should never contain a given user's NID. Always use a generic department name or first and last name.

DEFINITIONS:

DKIM: DomainKey Identified Mail is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain.

SPF: Sender Policy Framework (SPF) is an email-authentication standard that is used to prevent spammers from sending messages on behalf of a domain. With SPF an organization can publish authorized mail servers in DNS.

DMARC: Domain-based Message Authentication, Reporting & Conformance (DMARC), is an email authentication, policy, and reporting protocol. DMARC utilizes SPF and DKIM, adding context to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

Spoof: Sending mail on behalf of one or more user accounts within one of your organization's domains, or an external domain sending to your organization.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

RELATED DOCUMENTS:

- 4-006.2 *Broadcast Distribution of Electronic Mail* policy
- 4-014 *Procurement and Use of Cloud Computing and Data Storage Services policy*
- NIST 800-177 – Trustworthy Email
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
- UCF Mass Email Guidelines
  - https://infosec.ucf.edu/awareness/faculty-staff-security-guidelines/mass-email-guidelines/

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu	

Revision Date	Summary of Change

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL

(For use by the Information Security Office) Standards

Number: 109

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv chrisv dc=edu, dc=ucf, dc=net, ou=People, cn=chrisv, email=Chris.Vakhordjian@ucf.edu 2020.03.10 10:22:11 -04'00' Date: _____

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution