THE LeMoyne-Owen COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

LeMoyne-Owen College

IC2 - Email Authentication

March 16, 2020

IC2 - Email Authentication

Email sent from organization domains are authenticated using standard protocols such as SPF, DKIM and DMARC.

LeMoyne-Owen College Email Authentication

1.0 Purpose

To protect the LeMoyne-Owen College brand and potential phishing targets. When email goes out from LeMoyne-Owen College, the general public will tend to view that message as an official policy statement from LeMoyne-Owen College. If a message is not authenticated through SPF, DKIM and DMARC, a third party could spoof the organization's domain(s) and send malicious and erroneous email messages as if they were from the organization.

2.0 Scope

This policy covers the need to authenticate any email sent from LeMoyne-Owen College email addresses and applies to all employees, vendors, and agents operating on behalf of LeMoyne-Owen College.

3.0 Policy

3.1 SPF - Sender Policy Framework

Sender Policy Framework (**SPF**) is an email validation protocol designed to detect and block email spoofing by providing a mechanism to allow receiving mail exchangers to verify that incoming mail from a domain comes from an IP Address authorized by that domain's administrators. SPF should be set up for all of your email sending hosts.

3.2 DKIM - DomainKeys Identified Mail

DomainKeys Identified Mail (**DKIM**) is an email **authentication** method designed to detect email spoofing. It allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain and signed cryptographically by that domain with it's private key. DKIM should be set up for all of your email sending hosts.

3.3 DMARC - Domain-based Message Authentication, Reporting and Conformance

Domain-based Message Authentication, Reporting and Conformance (**DMARC**) is an email-validation system designed to detect and prevent email spoofing. It is intended to combat certain techniques often used in phishing and email spam, such as email messages with forged sender addresses that appear to originate from legitimate organizations. DMARC counters the illegitimate usage of the exact domain name in the From: field of email message headers. DMARC reports provide details about the effectiveness of your DKIM and SPF implementations. DMARC should be set up for **ALL** of your domains; for domains that email is sent from and for domains that are not used for email (defensive).

3.4 Monitoring

LeMoyne-Owen College regularly reviews and updates organization domains, 3rd party senders, and authentication settings to ensure that all domains are authenticated. Use of a DMARC analytics vendor is highly recommended.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Controls

IC2.0 - SPF Email Authentication

SPF records are added to domains that the organization sends email from. Other organizations that send email on our behalf are included as well.

IC2.1 - DKIM Email Authentication

DKIM records are added to the domains that the organization sends email from. Other organizations that send email on our behalf use the same key.

IC2.2 - DMARC Email Authentication

DMARC records are added to all domains owned by the organization to protect domains that are not used to send email and to monitor SPF and DKIM implementations on domains that email messages are sent from.