IT USE GUIDELINE

UA E-Mail Origination and Forwarding

Recommendations regarding the origination or forwarding of UA business-related email.

Effective as of: **9/1/2014**

Sponsor and Approvers:

Scott Montgomery, Ashley Ewing - Sponsors

John McGowan, IT Governance - Approvers

Status of Guideline: **Published**

Audience:

This IT Guideline should be observed by:

Students ☐ Faculty ☒ Staff ☒

Contractors/suppliers ☐

Other (specify) ☒ Others using UA email accounts.

Statement of need and purpose:

It has been common practice in the past to conduct university business using personal or other non-UA email accounts. Such activities include but are not limited to correspondence with students. This practice represents a risk to university interests and potential personal liability to those doing so. Non-UA email hosting services vary with respect to their privacy policies and security practices. In some cases, email may be inspected or searched for marketing or research purposes by them or their authorized agents. In other cases, email may not be securely maintained and so may be subject to exposure to unauthorized third parties. In some situations, UA email may be considered evidence in civil or criminal cases. Using personal or other non-UA email accounts for university activities can, therefore, place your personal email at risk of being viewed as evidentiary as well. Such activities include forwarding of UA email to a personal or 3rd party hosted account or originating UA-related email from a personal or 3rd party hosted email account.

Guideline:

All university-related email correspondence, including all correspondence to students, vendors, or other university business associates, sent by UA faculty or staff, should originate from a UA hosted email account. UA-related emails should not be forwarded to personal or 3rd party hosted email accounts.

Compliance:

Compliance to Guidelines is voluntary but recommended. Not adhering to guidelines can cause disruption to services, security exposures, and/or adverse impacts to other users. Enforcement of guidelines is addressed when deviations cause issues for others or result in known and significant security exposures and are handled through the organizational management structure.