UB IT CENTRAL EMAIL POLICIES AND PROCEDURES

Category: Information Technology
Responsible Office: Enterprise Infrastructure Services
Responsible Executive: Chief Information Officer

Date Established:
Date Last Revised: **3/26/2012**
Date Posted to Library: 4/12/2012

Note: These policies and procedures do NOT apply to UBmail accounts powered by Google (Google Apps for Education Accounts).

Summary

A collection of policies and procedures for Central Email such as; spam filtering, forwarding, retention etc. that do not apply to UBmail accounts powered by Google.

Policy

BACKGROUND

UB provides central email accounts primarily to employees and to select groups of students to support the teaching, learning and research mission of the university. The purpose of these policies is to

- Ensure that adequate resources are available to all of our account holders to carry out their academic and professional responsibilities
- Provide a proactive central spam filtering service for the UB community
- Prevent situations where non-UB email providers block the delivery of all UB email to their systems.
- Inform users of their responsibilities in using the central email system
- Inform users about the release of email as public records under New York State Freedom of Information Laws and the release of email under new federal e-discovery rules
- Describe the conditions when the contents of an email account will be provided to others in the case of a deceased individual.

DEFINITIONS

New York State Freedom of Information Laws – also known as FOIL governs rights of access to government records.
Federal e-discovery Rules – the federal court system can rule for the disclosure and production of electronically stored information used as evidence in federal civil lawsuits.
SPAM – is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.
Email Filter – is the processing of email to organize it according to specified criteria. Most often this refers to the automatic processing of incoming messages, but the term also applies to the intervention of human intelligence in addition to anti-spam techniques, and to outgoing emails as well as those being received.

Policy and Procedures

In order to manage spam proactively, all new UB central email accounts will be created with spam filtering enabled. Inbound messages will be scanned and rated, and messages rated as having an 80% or higher probability of being spam will be quarantined. Messages rated at 99% are dropped. See UBmail SPAM quarantine service page for details.

Note: UBmail powered by Google accounts utilize Google's SPAM filtering mechanisms.

Outgoing Email messages, originating from UB servers or forwarded from elsewhere, with a spam rating of 80% or more will be dropped (i.e., will not be sent), since the email is highly likely to be originating from a compromised or misconfigured machine on campus acting as a spam bot. This measure is being implemented to prevent UB from, becoming gray- or black-listed by ISPs, blocking delivery of all UB email to their systems.

Central Email Forwarding Policy and Procedures

In order to manage spam proactively, email forwarding that negatively impacts our central email servers will be disabled/removed.

Central Email Forwarding Policy and Procedures

In order to manage spam proactively, email forwarding that negatively impacts our central email servers will be disabled/removed.

- Central email forwarding addresses of students will be preserved for 6 months after their graduation/departure.
- Forwarding addresses of faculty and staff who leave UB employment will be preserved for a time period ranging from one day to 6 months following the date of their departure, depending on the nature of their departure (resignation, termination).
- Retirees may continue to keep their UB IT accounts and use UB central email services including forwarding if they wish.
- Each month a probe of all forwarded addresses of non-affiliated users (students who have left the university; employees who have resigned or been terminated) will be conducted. The probe will require an acknowledgement from the user. If no acknowledgement is received to the probe within 30 days, the email forwarding will be removed.
- In order to manage spam proactively, email forwarding that negatively impacts our central email servers will be disabled/removed.

Retention of Deleted Email

UB retains email centrally for disaster recovery purposes alone. Deleted messages (messages in the trash/recycle bin) are retained for 7 days. Originators and recipients of email are responsible for identifying and saving documents that must be retained in order to comply with federal, state, or local laws and to meet operational, legal, audit, research, or other requirements.

Email with Forged Header Information

Sending email with forged header information (specifically with a forged *FROM* line) is prohibited. The central email service will not accept email for nonexistent UBIT account names.

RESPONSIBILITY

User Responsibilities

The UB central email system is used as an official channel of communication. Faculty, students, and staff are responsible for reading UB email regularly for official University communications. Those who forward their UB email to a non-UB account are responsible for managing their disk quota for the non-UB account to ensure that there is enough disk space for new email. They are also responsible for keeping their email forwarding addresses up-to-date, ensuring that UB email is being forwarded to a functioning email address. Email forwarding addresses can be updated at: http://www.buffalo.edu/ubit/service-guides/email/ubmail-central-email/managing-your-ubmail--central-email-/forwarding-your-email.html. There is no mechanism for setting or updating an email forwarding address once the account has been deactivated.

The use of UB email systems is also subject to the normal requirements of legal and ethical behavior within the University community. Policies and regulations that apply to other forms of communication at the University also apply to email. Please see the Computer and Network Use Policy for more information on acceptable use of University IT resources. UB provides email systems for activities and functions supporting its mission of teaching, learning, research and discovery, and service.

Email: UB Employee Responsibilities

UB employees need to be aware that law and policy relating to the use of state resources make it important to separate work and personal email & files. Upon termination or resignation, an employee's email account will be terminated and all information in your UB mailbox not retained by the University will be deleted.

It is recommended that UB employees obtain an email account with one of the many services available for their personal email. UB email communications may be subject to public access under NY State FOIL and federal & state e-discovery rules.

Email: Public Records, E-discovery, and Privacy/Security

Email may contain official University correspondence as well as non-official correspondence, attachments, and forms transmitted electronically. It is important for all users to note that copies of email messages, including personal communications, may be released to the public under the New York State Freedom of Information Law. In addition, all email messages including personal email may be subject to and released in response to various government and court-ordered legal actions. New federal rules regarding discovery of electronically-stored evidence require the preservation and production/disclosure of any electronic evidence that is regularly and routinely available, including email messages, when there is an expectation of litigation.

Email: Deceased Individuals

In order to protect the privacy of third parties and to ensure that the University meets its obligations to all students under the Family Educational Rights and Privacy Act (FERPA), a deceased student's email will be provided only to law enforcement for investigative purposes, provided the request is made within the normal email retention period.

In order to protect the privacy of third parties, email belonging to deceased faculty, staff, or volunteers will be provided only to law enforcement for investigative purposes or to the individual's immediate supervisor exclusively for the purpose of continuity of University operations, provided the request is made within the normal email retention period.

Applicability of Policy

This policy applies to all University data regardless of its medium and/or form, and to all those who handle University information (faculty, staff, students, third party contractors, and any others).

Policy Review and Update

The Chief Information Officer or his designee will periodically review and update this policy as needed. Questions concerning this policy should be directed to the Office of the Associate VP for Information Technology.

Compliance

Violations of this policy will result in appropriate disciplinary measures in accordance with University policies, applicable collective bargaining agreements, and state and federal laws.

Contact Information

Director of Enterprise Infrastructure Services
305c Computing Center
University at Buffalo
saira@buffalo.edu
(716) 645-2298

Related Information

University Documents:

- UB Computer and Network Use Policy
- UB Email for Mass Digital Communications Policy
- Management and Retention of Email