Issued by: Division of Information Technology, Office of the CIO

Replaces:

Date of Issue:

Email D 106

POLICY

Network resources, including email accounts, are available to University students, faculty, and staff in furtherance of the University’s education, research, public service and health care missions. Access to email service may be provided to other users only on specific approval from DoIT’s Chief Information Officer (CIO), in accordance with SUNY policy.

1. Conditions for Use of University Email Accounts: Email accounts provided by the University to employees are intended for University business.

   The University does not guarantee the confidentiality of email services. Although every effort is made to preserve the integrity of the University email system, users should be aware that the interception of email messages on shared networks is possible. Email messages should be appropriately protected, using available encryption technologies.

   The owner of an email account is responsible for its use and is presumed to send all email actually sent from that account. Users may not alter an email address to disguise or block the identity of the sender.

   Email passwords and other credentials may not be shared. Email systems that rely exclusively on a User ID/password combination for security shall require periodic password changes to insure that the account maintains its integrity.

   Users may not view, copy, alter or destroy another’s email without permission unless authorized or required to do so by law or policy.

   Email may be scanned automatically for malicious content (viruses, spam, phishing attacks) and deleted without warning.

2. Inspection, Monitoring or Disclosure of Email: Email records residing on University-owned machines belong to the University, may be audited by DoIT at any time, and may be subject to disclosure to a third party, including review by authorized law enforcement personnel.

   Email accounts are subject to review and disclosure without notice when required by law, where a violation of law or University policy may exist, where there is a risk of spoliation, bodily harm, property loss or damage, where the University’s mission is jeopardized or during routine system administration.
3. Bulk Transmissions:

   A. Broadcast Emails Broadcast messages (formatted for distribution to more than 100 individual recipients) or
      email messages to the entire or specific segments of the University community require pre-approval from the
      President, Vice Presidents, Provost or the CIO. Advance notice of at least two business days is required.
      Communications from instructors and academic department or program chairs to current students in
      connection with instructional activity are exempt from this provision.
      Due to server demand and increased risk of viruses, distributed messages must be short and contain no
      attachments. Unless specifically authorized by the CIO, distribution of an email message to more than 100
      individual recipients is prohibited.

   B. Distribution Lists Distribution lists shall be developed for a specific purpose. Users who develop personal
      distribution lists must insure, prior to distribution, that each recipient is willing to receive the communication.
      Use of these lists for other than stated purposes is not permitted.

4. Retention of Email Records: DoIT email services are backed up daily. Email messages stored on a server within
   the backup cycle may be retrieved even if the user has deleted them. See DoIT 101. Local copies of email files are
   the user’s responsibility.

5. Closing an Email Account: Employee email accounts are shut down on the date of separation from the
   University.

   Employees who retire from the University may continue to use email accounts for a period of three (3) years after the
   retirement date. Thereafter, retirees may apply to their former department to sponsor the continuation of the account
   for a stated purpose that supports the mission of the University.

   On separation from the University, former employees may request that email be forwarded to a non-University
   address for a maximum of six (6) months. This request may be granted in the discretion of the University. The
   employee’s department may request that the email account of their former employee be kept open for a maximum of
   2 months.

   Disposition of email sent to a suspended or terminated employee is determined on a case by case basis.

INQUIRIES/REQUESTS:

Office of the Chief Information Officer
Room 231, Educational Communications Center
632 - 9085