Brandeis University

Accessing Digital Content

Policy Statement

The content of email and files stored on a University computer or in an authorized user's email or network account may be viewed only by the authorized user, unless otherwise so designated by the authorized user. Access to digital content by others is prohibited unless the protocols described below are followed.

This policy sets forth the circumstances and process by which Brandeis University may access the content of electronic communications and files on University computer systems. It further defines boundaries for such access and in general establishes an organizational posture ensuring continuing respect for the privacy of the University community.

Applicability

This policy applies to all Brandeis faculty and staff and all digital or electronic resources maintained by the University.

Guidelines

The University's Chief Information Security Officer or Chief Information Officer is the steward for the data access process and is obligated to oversee and document its application.

All requests for data access must be directed to the Chief Information Security Officer or Chief information Officer.

Requests must come from the organizational head of a unit and that individual's immediate supervisor. For faculty this will typically be a department/program Chair and Dean or Dean and Provost. Requests may also be made by the General Counsel in situations where the University is required to comply with a subpoena or assist state or federal authorities in an investigation.

It is appropriate at the direction of the Security Officer for digital content to be preserved by the Security Office while a data access request is pending including before notification to the affected individual.

An individual whose University computer data or email account is being accessed will be notified and, normally, notice will be given as soon as is practical. However, notification may be made post access or entirely suppressed if necessary to comply with a legal instrument or other investigative constraint.

Conditions for disclosure

Note: Non-legally compelled access will be provided only as part of a University investigation authorized by the Provost, a senior manager reporting directly to the President, or the President, and evidence will only be provided to the appropriate investigative body within the University (e.g., HR for personnel matters), with the exception noted below.

In general, access may be approved for:

- Litigation and Legal Processes: legal Instruments such as search warrants, discovery requests, or subpoenas that have been reviewed by the General Counsel.

- Internal Investigations of Misconduct or Audit: internal investigations under the auspices of an investigative unit of the University or as part of a legal or financial audit.
- Life Safety: emergencies where access to content may help prevent bodily harm to a member or members of the University community. These will be initiated in consultation with the Brandeis Director of Public Safety/Campus Police.
- Business Continuity: absences impacting business continuity may result in a unit being given access to email or digital files. In these circumstances, care must be given to protect the privacy of the individuals affected and the confidentiality of the accessed materials. The University's Chief Information Security Officer will establish a process to ensure these protections.
- Business Continuity and ex-employees: Work-related digital content of faculty and staff accounts may be provided, upon request and approval by a dean, a senior manager reporting directly to the President, or the President, to the supervising unit after the termination of employment.
- System Maintenance and Security: staff supporting the University's technology infrastructure and its security may, in the performance of their jobs, access or witness otherwise confidential data as required.

At the discretion of the President, Executive Vice President or Provost, in consultation with the General Counsel, access may be granted on the authority of the President, Executive Vice President or Provost in order to address exigent or unforeseen circumstances.

Authorization for access to digital content may be provided by the consent of the user of the account accessed. When access is approved by the user no notification or additional documentation is required.

Records Management

The Chief Information Security Officer will maintain records of all requests, whether approved or denied, for a period of three years. An aggregate summary report, absent any personally identifying information, may be provided for purposes of internal audit upon request.

Definitions

Electronic Content - Any digital file or communication, including but not limited to email, voicemail, log file, authentication or authorization record, or document and associated metadata.

Users, Users' accounts - Faculty and staff of Brandeis University, including individuals in sponsored or visitor roles and any University provided accounts they may be granted as part of their affiliation with the University.

Systems - All services, computers, networks and devices owned, provided or administered by any unit of the University. This includes but is not limited to email services, file services, voice message services, digital storage devices and services, desktop computers, laptop computers and other mobile devices, and usage and access logs.

This policy is for general guidance only. It does not create an employment contract or any right to continued employment at Brandeis University. Brandeis University reserves the right to modify, revoke, suspend, terminate and or change any and all policies and procedures at any time, with or without notice.

Office of Human Resources
01/2018