Effective Date: **June 1, 2017**

**POLICY**

**EMPLOYMENT, ETHICS, INFORMATION MANAGEMENT, PRIVACY AND SECURITY, STUDENT LIFE**

# Access to Electronic Information Policy

RESPONSIBLE OFFICE

**Information Services and Technology**

Reviewed: April 2019 by CSIS Governance

## Overview and Scope

Boston University makes electronic systems, networks, and devices available to the community to carry out University business. Except as described in the Network Security Monitoring Policy, the University does not routinely access the content of users' electronic mail, calendar, files, or network access logs ("User Information") transmitted through or stored in systems, networks, or devices owned, leased or arranged for by the University or which the University possesses, has custody over, or controls ("BU Systems"). However, because access may be necessary in certain circumstances, this policy describes circumstances under which the University may access User Information and the processes and authorizations necessary for such access. This policy is intended only to establish internal standards and procedures governing such access. It does not create legally enforceable rights in members of

the BU community to privacy of data transmitted through or stored in University systems, networks, or devices.

In the event that a user's electronic information resides on a device owned by Boston Medical Center (BMC) or is the property of BMC, BMC policies and procedures shall govern.

# Permitted Reasons for Access

Access to User Information stored on BU Systems may be necessary to meet the University's obligations to preserve and provide electronic information in connection with legal proceedings, to investigate allegations of misconduct, to obtain business critical information when a user is unable or unavailable to provide consent, and to address threats to the University community or individuals in a timely manner.

## A. Legal Proceedings and Litigation

The University may access User Information in connection with threatened or pending litigation, and to respond to lawful demands for information in law enforcement investigations, other government investigations, and legal processes if authorized as described below.

## B. Internal Investigations of Alleged Misconduct

The University may access User Information in connection with authorized internal investigations of misconduct by members of the University community, provided that access has been authorized as described below in Section 3 and the authorizing person has weighed the need for access with other University values and determined that an investigation would advance a legitimate institutional purpose and that there is a sufficient basis for providing access. Examples of investigations that may necessitate access to User Information include, but are not limited to, allegations of conduct that would violate: the Code of Ethical Conduct, Research Misconduct Policy, Sexual Misconduct/Title IX Policy, Conditions of Use and Computing Ethics Policy, Policy on Unlawful Discrimination or Harassment, Consensual Relationships Policy, Violence Prevention in the Workplace, Protection of Minors Policy, Athletic Institutional Control and Responsibility, Code of

Student Responsibilities, and the Student Athlete Code of Conduct.

### C. Business Need

The University may access User Information (i) when such information is required to perform a critical, time sensitive function that is necessary for business continuity, such information cannot practically be obtained in another way, and the user is unable or unavailable to provide access to the information or to consent to the access, provided that access has been authorized as described below in Section 3 and the authorizing person has determined that access to the information would address a critical business need and that there is sufficient basis for providing access, and (ii) incidentally, in the course of providing information systems support, provided that the staff person who is providing such support is doing so as part of the staff person's job responsibilities.

### D. Safety Matters

The University may access User Information to deal with exigent situations presenting threats to the safety of the campus or to the life, health, or safety of any person.

## Authorization of Access

In any of the circumstances described above, an appropriate person, designated below, must authorize access (the "authorizing person"). In deciding whether to approve access, the authorizing person should consider whether there are reasonable, effective, alternative, timely means to obtain the information. In all cases, access must comply with applicable legal requirements. An authorization shall apply only to the particular situation and user or users and is limited to the approved scope of access. Any other instance of access or any requested change in scope from that approved in the initial authorization must be separately authorized.

The user may always authorize access to his or her own User Information. Authorization should be provided in writing and preserved with the access request.

In the absence of authorization by the user, the following applies:

A. In connection with litigation, legal processes, law enforcement or federal or state

agency investigations, or to preserve User Information for possible subsequent access in accordance with this policy, the Office of the General Counsel must authorize access in writing.

B. Access to User Information for purpose of internal investigations of alleged misconduct is authorized as follows:

1. If the user is a faculty member or if the user cannot be identified in advance, the Provost or his or her designee must authorize access in writing.

2. If the user is a staff member or other affiliate, the Chief Human Resources Officer or his or her designee must authorize access in writing.

3. If the user is a student, the Dean of Students or his or her designee must authorize access in writing.

4. If the user is an alumnus only, the Senior VP for Development and Alumni Relations or his or her designee must authorize access in writing.

As a general rule, the designated University official should confer with the Office of the General Counsel before authorizing access, and consult, as appropriate, with the relevant academic Dean or Vice President.

Information Services and Technology will maintain a log of all instances in which access was authorized in connection with internal investigations of misconduct.

C. To access User Information to obtain business critical information that cannot practically or timely be accessed another way: (i) in the case of a staff member, the director of the business unit in which the user is or was employed must authorize access in writing, and (ii) in the case of a faculty member, the Dean of the school or college in which the faculty member holds an appointment must authorize access in writing.

D. To access User Information in exigent situations involving a threat to campus safety or the life, health, or safety of any person, the Office of the General Counsel or the Boston University Chief of Police must authorize access.

# Notice

When the University intends to access a current user's User Information, notice ordinarily should be given to that user at the time of access or as soon thereafter as reasonably possible. Current users include retirees who maintain an active "bu.edu" email address.

However, notice is not required where the University is legally constrained or restricted from providing notice. Contemporaneous notice is not required in cases where there is insufficient time, where giving notice would otherwise interfere with an effective response to an emergency or other compelling need (e.g., at a stage of an internal investigation where giving notice may compromise the investigation), or where it is impractical. In such cases, notice will ordinarily be given as soon as practical. In addition, the University need not notify users who are deceased or who are no longer affiliated with the University. The designated authorizing person will determine whether notice is required or may be delayed for one of the reasons given in this section, in consultation with the Office of the General Counsel.

# Scope of Access

Whenever practicable, the authorizing person will take reasonable steps to limit the access to that which is reasonably necessary to achieve the University's purpose. These limits will vary depending on the circumstances; limits may include, for example, targeted search terms or time parameters.

Participation in the search, and access to the User Information, should be limited to those University personnel or University agents with a legitimate need to be involved.

# Effective Date

The Policy on Access to Electronic Information takes effect 6/1/17.

# History

The Policy on Access to Electronic Information was drafted by the Office of Information Services & Technology and the Office of the General Counsel, reviewed by the University Council Committee on Faculty Policies, and recommended for approval by the full University Council. It was approved by the University Council on 5/17/17.

END OF POLICY TEXT

Categories: Employment, Ethics, Ethics and Activities, Faculty, Information Management, Information Technology Use, Access, and Security, Privacy and Security, Student Life, University Policies Affecting Student Life Keywords: allow, permissible, permitted, protocol