Effective Date: **May 23, 2023**

POLICY

ETHICS, INFORMATION MANAGEMENT

Acceptable Use of Computing Services Policy

RESPONSIBLE OFFICE

Office of the Vice President Information Services and Technology

Purpose

This policy defines acceptable use of the computing services provided by the University as well as the responsibilities of users and requirements to which all clients must agree as a condition of being granted access to the University's computing services. It is a replacement of the current Conditions of Use and Policy on Computing Ethics.

Covered Parties

The revised policy applies to all persons who use the University's Computing Services as defined below, described herein as "Clients".

Defined Terms

“Account” refers to the combination of data and Computing Services that can be accessed by an individual once they have proven their digital identity.

“Computing Services” means computer systems, personal devices, networks, and all forms of software, firmware, operating systems, application platforms, and digital content they provide or host, which are owned, leased, or arranged for by the University or which the University possesses, has custody over, or controls. Computing services include all technology used to provide and store “User Information”, as defined in the Access to Electronic Information Policy. Computing Services also include cloud- or internet-based services arranged for by the University or generally available cloud- or internet-based services used to conduct University business or store University data.

University Policy

Boston University’s Computing Services are intended to be used to facilitate the education and research missions of the University and support University operations. All Clients of these services have the responsibility to use these resources in an efficient, ethical, and legal manner in accordance with their intended use and assigned access rights, to ensure that the University’s computing services remain available without interruption to all Clients.

Use of the University’s Computing Services in connection with university activities and minor personal use is a privilege extended to various members of the University community; it is not a right. By using the University’s Computing Services, all Clients (i) acknowledge and agree to comply with, be subject to, and grant the University the right to implement, this Policy; (ii) agree to comply with applicable laws and other University policies, (iii) agree to refrain from engaging in any activity that is inconsistent with the University’s tax-exempt status or that would subject the University to liability; and (iv) acknowledge and agree that the University has made no representation as to the privacy of any communication or data stored on or sent through these services. In addition, upon creation of a Boston University computing Account, all Clients agree to the following conditions of use:

1. Clients must use only those Computing Services to which the University has

authorized their access, and only for the purposes for which such use was authorized. Unauthorized use of Computing Services, whether by providing false or misleading information for the purpose of accessing computing services or otherwise, is prohibited. Clients also must not use University Computing Services to gain unauthorized access to computing services of other institutions, organizations, or individuals.

2. Clients must not give their authentication credentials (passwords, multifactor tokens, etc.) for individual University Accounts to any other person for any reason. Clients must take all reasonable precautions to secure their credentials from misuse, including selecting a unique, strong password and complying with the requirements of the Identity and Access Management Policy as to the strength of such password and how frequently it should be changed. Clients should use appropriate delegation features if shared access to e-mail and calendars are required. Clients are responsible for all uses of their individual University Accounts.

3. Use of Computing Services, including the campus network, for more than minor private purposes or any commercial purposes is prohibited.

4. Clients must not use the University's Computing Services for any unlawful purpose, including but not limited to the collection, installation, or distribution of fraudulently or illegally obtained files or software.

5. Clients' use of external networks or services – including cloud services – must comply with all applicable acceptable use policies, whether published by the University or by the organizations providing those networks or services.

6. Clients must not access, alter, copy, move or remove proprietary information or software without prior authorization from the appropriate University data trustee, security officer, or other responsible party. Clients must not copy, distribute, display, or disclose third-party proprietary software without prior authorization from the licensor. Clients may not install proprietary software on systems not properly licensed for its use.

7. All devices used to access University data or networks must conform to all University policies including the Data Protection Standards. It is the responsibility of the device owner to secure personally owned devices.

8. Clients must not use any computing service:

    - For activities that are illegal or violate University policies or applicable codes of conduct;
    - To block or otherwise interfere with access of other authorized users to any University computing service;
    - To incite imminent lawless action;
    - To harass, intimidate or threaten any person, whether within or outside the University;
    - To disrupt or interfere with the University's ordinary activities;
    - In a manner that is otherwise directly incompatible with the safety of the community or the functioning of the University;
    - To send unauthorized mass mailings or unsolicited advertising;
    - To damage any system, material, or information belonging to another party;
    - To intentionally intercept electronic communications or otherwise violate the privacy of others or access information belonging to or intended for another party;
    - To intentionally misuse system resources or make it possible for others to do so;
    - To load software or data from untrustworthy sources onto University systems; or
    - To infringe on a third party's copyright.

University's right to take necessary action

To ensure the integrity of the University's Computing Services and to protect against unauthorized or improper use of those services, Boston University reserves the right, without notice, to investigate reports of misuse to determine the validity of those reports and identify the nature of the issue. Investigations shall be conducted in accordance with the Access to Electronic Information policy and the Cyber Incident Response Policy. The University acknowledges that conducting investigations of suspected misuse of Computing Services as outlined above may require Information Security (Infosec) to examine system, application and network logs collected in connection with the operation of University Computing Services and use other network monitoring technologies, as outlined in the Network Security Monitoring Policy, in order to ascertain the scope and severity of the alleged misconduct. Infosec personnel shall conduct investigations according to these three principles:

1. All investigations will be initiated based upon credible intelligence, which may include a variety of human and electronic data sources and performed by trained BU or BU-

contracted personnel.

2. Investigations will be impartial and will be conducted in a way that preserves privacy to the extent possible.
3. If an investigation points towards the involvement of a University community member or requires non-emergent detailed or prolonged examination of an individual's activity or access to personal data, the process described in the appropriate section of the Access to Electronic Information Policy shall be followed to ensure that appropriate authorization is received before such information is accessed.

Further, the University reserves the right to take the following steps (which may be taken without prior notice in order to prevent imminent damage to University Computing Services or to the data of other users):

i. limit or restrict any individual's use, and view, copy, remove or otherwise alter any data, file, or system resource, based on a reasonable belief that continued use of such data, file or resource is likely to negatively impact the confidentiality, integrity, or availability of the University's shared computing resources or to cause the University to be out of compliance with the terms of an applicable license under which such resource is available;

ii. enforce security controls to preserve the confidentiality, integrity, or availability of the University systems or networks. These controls may affect the storage, transmission, and access of confidential and protected information in accordance with University policies and state, and federal laws or regulations; and

iii. restrict access to internal or external resources based upon perceived risk to the University systems or networks.

The University is not responsible for loss of data or service interruptions resulting from its efforts to maintain the privacy and security of University Computing Services, system malfunction, or any other cause.

Procedures

Report concerns to BU Information Security, the IT Help Center or Internal Audit & Advisory Services. Violations of this Policy may result in (a) restriction or removal of some or all

privileges to use Computing Services and (b) disciplinary actions through appropriate University processes, specific to students through the Dean of Students, staff through Human Resources, and faculty and other users through Human Resources and/or the University Provost's Office. The University reserves the right to amend this Policy at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable laws.

Responsible Parties

Information Security, Information Services and Technology
179 Amory Street
Brookline, MA 02446
617-353-4357
ithelp@bu.edu

Related Policies and References

Access to Electronic Information Policy, effective June 2017
Network Security Monitoring Policy, effective June 2017, amended January 2018
Data Protection Standards

- Identity and Access Management Policy, effective January 2011, amended April 2019
- Minimum Security Standards, effective January 2011, amended April 2023

Policy History

This policy replaces the Conditions of Use and Policy on Computing Ethics, which had been approved July 15, 2014.

END OF POLICY TEXT

Additional Resources Regarding This Policy

History

This Policy replaced the Conditions of Use and Policy on Computing Ethics on May 23, 2023.

Related Policies and Procedures

- Access to Electronic Information Policy, effective June 2017
- Network Security Monitoring Policy, effective June 2017, amended January 2018
- Cyber Incident Response Policy
- Data Protection Standards
- Website Policy
- Listing of related BU TechWeb Policies

This Policy is also a part of the Faculty Handbook section on Ethics and Activities.

Categories: Acceptable Use, Ethics, Faculty Handbook: Ethics and Activities, Information Management, Information Technology Use, Access, and Security, Student Codes of Conduct, University Policies Affecting Student Life, Workplace Keywords: Acceptable Use, accommodation guide, computing service, computing services, copyright, cyber incident, cyber incident response, cyber response, device, devices, E-mail, Email, network, networks, software