Effective Date: **May 23, 2023**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Cyber Incident Response Policy

RESPONSIBLE OFFICE

Office of the Vice President Information Services and Technology

Purpose

Boston University has a responsibility to ensure the security of its information systems by defending its computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks and protecting the confidentiality, integrity, and availability of data. The purpose of the policy is to authorize Information Security to investigate and respond to Cyber Incidents that pose an immediate threat to the confidentiality, integrity, or availability of Computing Services.

Covered Parties

This policy applies to all students, faculty, staff, guests, and other persons who utilize university Computing Services.

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 data. [See *Acceptable Use of Computing Services Policy*]

"Cyber Event" is any event which may impact on the security of data and Accounts. Events occur regularly, including benignly mistyped passwords, Cyber Incidents, Violations involving Computing Services, and other reported vulnerabilities in information systems. Events may be detected and reported in a variety of ways, including alerts from security technology, reports from the community, law enforcement, or other trusted sources, through e-mails and ticketing systems, social media, news stories, interpersonal interactions, and phone, Teams, or Zoom calls.

"Cyber Incident" is one or more Cyber Events where a party gains, or attempts to gain, unauthorized access to Computing Services, data, or an Account, using methods such as "phishing", hacking, denial of service, malware including ransomware, or unauthorized use of a password. These incidents pose an urgent threat to the security of the University's Computing Services and require immediate investigation to mitigate the risks.

"Major Security Incident" is a subset of Cyber Incidents that has or is likely to gain campus or university scope, has or is likely to impact the privacy of personally identifiable information maintained by or for the University, has significant reputational or financial risk for the University, or exceeds the available resources to mitigate.

"*Violation using Computing Services*" occurs when an authorized party uses University Computing Services in a manner that violates applicable law or University policy, such as pirating software or resources from another party, sending inappropriate email messages that are threatening or harassing as defined in University policies,

misuse of data, or research misconduct involving research stored on our computers.

University Policy

Cyber Event Reporting

All members of the Boston University community have an obligation to report Cyber Events that are or could lead to a Cyber Incident or Violation using Computing Services in a timely fashion. The official method for individuals to report Cyber Events is to send notice of such events and relevant information to the IS&T Service Desk via ithelp@bu.edu.

Delegation of Authority

This policy establishes Information Security, under the leadership of the Chief Information Security Officer, as the lead organization in conducting the investigation of any Cyber Incident involving Computing Services, Accounts, or data and describes the University's approach for responding to such incidents.

Information Security may assist in the technical investigation of Violations using Computing Services but will not lead or authorize those investigations. Investigations will be led by the Responsible Office(s) listed in the applicable policy document, using authorizations derived from the Access to Electronic Information Policy. The Vice President of Information Services & Technology may authorize Information Security to investigate violations of its policies, such as the Acceptable Use of Computing Services Policy, under the same conditions.

Privacy During Investigations

The University acknowledges that conducting investigations of suspected Cyber Incidents may require Information Security to examine system, network, and application logs and similar data collected in connection with the operation of University Computing Services, to ascertain the scope and severity of an Incident and its source. Such authority is appropriate to support the University's interest in ensuring "appropriate and legal use and performance of the network"

but should be implemented in a manner that preserves the privacy of the Account holder to the extent possible. The scope of the investigations may vary significantly but examples of actions may include searching logs for a specific e-mail that was sent at specific time and date or scanning an individual's files or devices for malware. Protections for privacy include limiting the number of individuals involved in an investigation and constraining search terms and time periods reviewed, as appropriate.

Information Security will continue its investigation until the threat to Computing Services and Accounts is contained. If during an investigation Information Security determines that a community member may be involved and thus violating university policy, the matter will be referred to the Responsible Office for the relevant policy. Information Security will not use a Cyber Incident to investigate unrelated policy violations or an individual's activities that do not threaten the security of Computing Services except to the extent required by law to bring such activities to the attention of law enforcement. If an investigation 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 before accessing such information. Information Security may copy or freeze an Account and its associated data to ensure that relevant information is not deleted before it can be examined.

If a review by Information Security leads to the conclusion that the Account of a BU individual was compromised by an external entity and no University-affiliated individual was responsible for such compromise, Information Security has the authority to share both the determination and the information used to support that determination with the Boston University Police Department (BUPD) in support of a BUPD-led investigation. Absent exigent circumstances, Information Security will provide notice to and seek consent by the Account holder before the investigation proceeds. Information Security is also authorized to share non-personally identifiable information related to Cyber Incidents with other entities, including national Information Sharing and Analysis Centers and law enforcement, for the general protection of the Internet.

Key Roles

(i) The Information Security **Security Operations Center (SOC)** will be responsible for the initial review and correlation of reported security events, prioritizing them, and determining which warrant escalating to the Incident Response Team (IRT) for further

investigation.

(ii) The **Incident Response Team (IRT)** is responsible for initiating the Incident Response Plan detailed below. The standing membership of the Incident Response Team (IRT) shall be members of Information Security designated by the Chief Information Security Officer and will incorporate additional members of Information Security, IS&T, and the university community on an ad-hoc basis according to the nature of the incident and required skills.

(iii) The Chief Information Security Officer shall define a cross-functional **Senior Incident Management Team (SIMT)** of university leadership that will provide oversight and be able to bring additional resources to aid in response during a major incident.

Procedures

The Chief Information Security Officer, with review and approval from the Common Services and Information Security Governance Committee, shall define high-level Incident Response Plans for responding to Cyber Incidents within the constraints of this policy.

Responsible Parties

Information Security, Information Services and Technology
930 Commonwealth Avenue 2nd Floor
Boston, MA 02215

Related Policies and References

Access to Electronic Information Policy, effective June 2017

Acceptable Use of Computing Services Policy, effective May 2023

Policy History

This is a new Policy drafted in February 2023 to codify and standardize incident response

policy and procedure. It is based on an existing Data Breach Management Plan that has been in use since 2011. The Policy passed in May of 2023.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies and Procedures

- Acceptable Use of Computing Services Policy, *effective May 2023*
- Access to Electronic Information Policy, effective June 2017
- Network Security Monitoring Policy, effective June 2017, amended January 2018
- Data Protection Standards
- Website Policy
- Listing of related BU TechWeb Policies

Categories: Information Management, Privacy and Security Keywords: breach, breach team, cyber incident, cyber incident response, data breach, incident response, Incident Response Team, irt