Effective Date: **June 1, 2017** Revised: **January 12, 2018**

POLICY

ACADEMICS, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Network Security Monitoring Policy

RESPONSIBLE OFFICE

Office of the Vice President Information Services and Technology

Reviewed: April 24, 2024 by CSIS Governance

Overview and Scope

Boston University Information Security is charged with protecting the University's electronic information assets, including by performing ongoing, routine network security monitoring and using technologies to detect and/or prevent network intrusion. Certain laws and regulations also contain security standards that may require the University to engage in network monitoring and reporting for cyber incidents. This policy describes the technologies in place, the principles for protection of individual privacy, access and retention controls for the data collected or stored, change management processes, and auditing and reporting requirements for the use of network monitoring technologies.

Network Monitoring Technologies

Network monitoring technologies examine network traffic as it passes specific points in the

network and may take action to record, alter, or block the traffic in order to protect the sender or the recipient.

Only Information Security is authorized to deploy and operate these technologies on a routine basis; Information Services & Technology (IS&T) and its IT partners may deploy and operate these technologies for short-term diagnostic purposes. Any other deployment or operation of network monitoring technologies that will expose traffic other than that of the individual operating the technology must be approved in advance by Information Security. Depending on the circumstances, review by the Provost or their designee, Office of the General Counsel (OGC) and/or Institutional Review Board (IRB) may also be necessary.

Information Security may use the following monitoring technologies on the Boston University network:

- Intrusion Detection
- Intrusion Prevention
- Firewalls
- Network layer antivirus and anti-malware
- Network layer advanced threat protection
- URL/IP-based reputation filtering
- Data Loss Prevention
- Netflow traffic monitoring

A description of how and where technologies are deployed will be furnished to the Common Services and Information Security (CSIS) Governance Committee upon request.

Commitment to Data Privacy

Information Security shall take reasonable means to preserve data privacy by adhering to the following principles:

- At no time will Information Security monitor or examine network traffic for any purpose other than protecting the information assets of the University and ensuring appropriate and legal use and performance of the network.
- Use of network monitoring technologies to meet the University’s obligations to preserve and provide electronic information in connection with legal proceedings, to investigate

allegations of misconduct, and to address threats to the University community or individuals in a timely manner is governed by the Access to Electronic Information policy.

- Information Security will not deploy technologies for the purpose of subverting the security of otherwise encrypted communications unless it has obtained the prior approval of the unit(s) affected.
- Information Security will capture and retain network traffic as permitted under the Access to Electronic Information policy and may capture and retain small amounts of network traffic related to specific vulnerabilities to identify security events or confirm a security incident, collect aggregate statistics about network use, and share de-identified or aggregate statistics with peers and information security analysis centers.
- Information Security's determination that access to an application or website should be allowed or disallowed will be based upon cybersecurity risk, not the content of the application or website. Any access prohibitions relating to website or application content shall be made by OGC.

Retention of Data and Access to Data

As used in this section, a "legitimate business need" means that an employee, based strictly on the employee's job responsibilities, has a specific and articulated reason to access information in order to carry out duties to the University.

1. Access to and retention of un-redacted data
   Network monitoring technologies produce logs that contain real-time, un-redacted, personally identifiable data. The Chief Information Security Officer may approve access to these logs in any form for IS&T staff with a legitimate business need. The Vice President of IS&T may approve access for non-IS&T staff with a legitimate business need. These logs may be retained up to 30 days.
2. Access to and retention of redacted data
   A redacted data set that does not include raw packet data but may still be personally identifiable, will be exported to the University's enterprise log management server. The Chief Information Security Officer may approve access to the enterprise log management server for BU technology support staff if there is a legitimate business need. Redacted logs may be retained for up to 365 days.
3. Netflow logs
   Netflow logs contain records of network traffic but no content and therefore no personally

identifiable information. The Chief Information Security Officer may approve access to Netflow logs for BU technology support staff if there is a legitimate business need. Netflow logs are retained up to 180 days.

4. Extracts and copies of logs
   Information Security may retain extracts from redacted or un-redacted logs related to security incidents for longer than 365 days and may share the extracts to resolve security incidents according to business need. Additional copies or exports of the logs are not permitted except as approved by the Chief Information Security Officer .
5. Other access to logs
   Use of any network monitoring data for any other purposes, including academic or research purposes, must be approved by the Chief Information Security Officer. Depending on the circumstances, review by the Provost or their designee, OGC and/or IRB may also be necessary.

Alterations to list of Network Monitoring Technologies

In the normal course, changes to the list of monitoring technologies above will require the prior approval of the CSIS Governance Committee. In emergent situations, the Vice President of IS&T may direct Information Security to implement additional features to protect the network until such time as the CSIS Governance Committee may be informed and provided the opportunity for review. This CSIS Governance Committee will review and update this policy accordingly.

Updates to Configuration of Network Monitoring Technologies

Network monitoring technologies require routine maintenance and updates to remain effective. The Chief Information Security Officer may determine that updated threat intelligence requires manual or automatic implementation of new rules within such technologies. Whenever practicable (such as when there is no emergent vulnerability), the Chief Information Security Officer will request review of the changes by the CSIS Governance Committee, which will review and update this policy accordingly.

Auditability

All manual changes to network monitoring technologies' configuration will be logged.

Reporting

A log of changes will be provided to the CSIS Governance Committee upon request.

Effective Date

The Policy on Network Security Monitoring takes effect 6/1/17.

History

The Policy on Network Security Monitoring 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

Additional Resources Regarding This Policy

Related Policies

- Data Protection Standards
- Sensitive Data Incident Response
- FERPA Policy
- Information Security Policy
- HIPAA Policy
- Listing of related BU TechWeb Policies
- Policy on Access to Electronic Information
- Digital Privacy Statement
- Conditions of Use and Policy on Computing Ethics

Related Procedure

- Policy Violation Notification Procedure

Categories: Academics, Information Management, Privacy and Security Keywords: control, defend, guard, safe