RESOURCE

Guidance on Use of Social Security Numbers and Other Personal Information

Social security and driver's license numbers are protected by state law. The University's Data Protection Standards explain what departments that collect, access, share, send, use or store this Restricted Use data must do to ensure that it is safe and secure.

EVERYONE

- **DON'T** request, access, use or store social security or drivers' license numbers unless there is a legitimate business need to do so and your department has confirmed that it complies with the Data Protection Standards for Restricted Use data.
- **DON'T** under any circumstances store sensitive information like social security or drivers' license numbers in Dropbox, Google Drive or any other service that has not been approved by Information Security.
- **DON'T** send or transmit social security or drivers' license numbers under any circumstances, unless you are authorized by your department and have a secure mechanism approved by Information Security for doing so.
- **DO** read the Data Protection Standards and be sure you understand how to secure sensitive information.
- **DO** help minimize risk. Be on the lookout for University forms (paper or electronic), emails, or old files (electronic or paper) that contain social security or drivers' license

numbers. If it doesn't seem necessary, say something. Ask your supervisor, Information Security, Compliance Services or Internal Audit for help determining whether it is appropriate for social security or drivers' license numbers to be in those places and, if not, how to safely and security destroy the information.

- **DO** report any suspected data breach to Information Security immediately in accordance with the instructions outlined on their webpage on Reporting a Sensitive Data Incident.

DEPARTMENTS THAT ACCESS, USE OR STORE SOCIAL SECURITY OR DRIVERS' LICENSE NUMBERS

- **DON'T** store social security or drivers' license numbers on unencrypted laptops, USB drives or portable devices.
- **DON'T** email or otherwise transmit social security or drivers' license numbers electronically. If it's absolutely necessary, contact Information Security to identify a secure way to do so. The University's encrypted email system may be used to send sensitive information to individuals outside of the University.

- **DO** contact Information Security or Compliance Services if you need help determining whether your collection or use of social security or drivers' license numbers is appropriate.
- **DO** make sure that social security and drivers' license numbers are stored in locked file cabinets or encrypted electronic storage.
- **DO** take special care to destroy social security and drivers' license numbers responsibly. Information Security provides simple explanations for destroying paper records, CDs, DVDs, files, storage devices, and the like.
- **DO** contact Sourcing & Procurement if you plan to buy or use software that will use or store social security or drivers' license numbers to ensure that the contract has appropriate protections in place to safeguard the information.
- **DO** report any suspected data breach to Information Security immediately in accordance with the instructions outlined on their webpage on Reporting a Sensitive Data Incident.

Consequences

- A data breach involving social security or drivers' license numbers may lead to identity theft or stolen funds. You don't want either of those to happen to you; you should do what you can to minimize the risk that it happens to others.
- If there is a data breach that involves social security or drivers' license numbers the University may be required to notify every individual whose information has been breached and may provide credit monitoring. In addition, the University may be required to notify state attorneys general and credit card companies about the breach. The department in which the breach occurs will participate in these efforts.
- Regulators may impose fines or penalties and individuals who are harmed may file lawsuits.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies and Procedures

- Data Protection Standards

Boston University Offices and HIPAA Contacts

- Information Security
  Information Security can help you keep data secure, reliable, and accessible.
- Internal Audit
  Internal Audit can help you determine whether you really need social security numbers and whether there's a more secure way to meet your business needs.
- Sourcing and Procurement
  Sourcing can help you find the right vendor and make sure the vendor is as careful

with sensitive data as we are.

Boston University Websites and Other Resources

- Reporting a Sensitive Data Incident Breach: The Incident Response Team (IRT) provides coverage 7 days a week, 365 days a year to respond to reported breaches of security. We encourage anyone who is aware of a potential security breach affecting Boston University accounts, computers, or networks to report all available information to the IT Help Center or call our hotline at 617-358-1100.