RESOURCE

Background Check Guidance

Information relating to criminal background checks, such as Criminal Offender Record Information (CORI), is protected by state law. The University's Background Check Policy explains how to conduct background checks and the BU departments authorized to do so. CORI records typically contain sensitive information, including Social Security Numbers as well as an individual's criminal activity. The University's Data Protection Standards explain what departments that have access to this Restricted Use data must do to ensure that it is safe and secure.

EVERYONE

- **DON'T** perform any type of background check unless your department has been authorized by Human Resources to do so.
- **DO** contact Human Resources with any questions related to background checks or CORI information.
- **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.

DEPARTMENTS THAT ACCESS, USE OR STORE BACKGROUND CHECK INFORMATION

- **DON'T** store background forms or information on unencrypted laptops, USB drives or portable devices.
- **DON'T** email or otherwise transmit CORI 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.
- **DO** make sure that only individuals who are fully trained in handling personally identifiable information receive and store CORI forms.
- **DO** ensure that CORI forms transmitted by fax are sent to a machine in a secured location.
- **DO** request that CORI forms sent by mail are addressed to the attention of the appropriate person.
- **DO** scan CORI forms with an individual scanning device attached directly to the computer to be used; avoid using multi-function devices.
- **DO** make sure to follow the Data Protection Standards.
- **DO** assign and train ONE individual in your department in charge to request, perform, store, and dispose of CORI information appropriately.
- **DO** make sure that CORI are stored in locked file cabinets or encrypted electronic storage.
- **DO** take special care to destroy background check information responsibly. Destroy CORI forms as soon as it has been submitted to Human Resources. 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 background check information to ensure that the contract has appropriate protections in place.
- **DO** report any suspected data breach to Information Security immediately.

Consequences

The Criminal Records Review Board that administers this information may issue orders for violation of the CORI law and regulations including civil fines of up to $5,000 per violation.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies

- Background Check Policy
- Data Protection Standards

Boston University Offices

- Human Resources

  Human Resources can help you with any questions about Background Checks for Protection of Minors compliance requirements.

- Information Security

  Information Security can help you keep data secure, reliable, and accessible. Report a data breach to the Information Security Breach Response Team

Reporting Breaches

There are several ways to report a breach depending on the nature of the incident and the type of information that may have been compromised. The following are the specific mechanisms.

- Reporting a Sensitive Data Incident: 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.
- Reporting a HIPAA Breach: If you believe HIPAA data (PHI) may have been accessed, used or disclosed by someone who is not authorized to do so, it is your responsibility to report the possible breach. Once you report the HIPAA Privacy and Security officers will be able to evaluate the situation and determine whether the situation qualifies as a breach.
  - How to report: HIPAA workforce members should notify their supervisor and/or HIPAA Component Contact. The HIPAA Contact then reports to IT Help Center (ithelp@bu.edu) or the HIPAA Officers (hipaa@bu.edu).
  - More information on how to report a HIPAA breach can be found at www.bu.edu/HIPAA.
- Reporting Breaches Related to Research: Breaches in confidentiality and other similar breaches related to research activity must be reported to the IRB using the Event Form, ordinarily within five (5) days of the PI learning of the incident.

Keywords: background check, background check guiance, background checks