PROTECTION OF REGULATED PRIVATE DATA POLICY

Category: Information Technology
Responsible Office: Office of the CIO
Responsible Executive: Chief Information Officer
Date Established: May 6, 2008
Date Last Revised: May 6, 2008
Date Posted to Library: 9/2/2011

Summary

University at Buffalo is committed to protecting *regulated private data*[1] in order to safeguard the privacy of community members; thus, reducing the very real threat of identity theft for community members, as well as minimizing UB's risk of violating State or Federal law and regulations. Incidents in which regulated private data have been compromised arise daily, and all UB community members need to understand the definition of regulated private data and take responsibility for protecting these data.

Policy

POLICY STATEMENT

It is the policy of the University at Buffalo to minimize access to and use of regulated private data in any form and to maximize the protection of these private data. Regulated private data include (1) bank credit/debit card numbers, (2) Social Security Numbers, (3) state-issued drivers' license numbers and state-issued non-drivers' identification numbers, (4) passwords and other computer access protection data, and (5) protected health information. University at Buffalo Standards for Securing Regulated Private Data establishes the requirements for protecting these data in any form and on any device, including the hard drives of digital printers and copiers.

COLLECTION, STORAGE, AND TRANSMISSION OF PRIVATE DATA

Collection, storage and/or transmission of regulated private data must be approved by the Information Security Officer in the CIO Office. Approval will be contingent upon the unit's demonstrated operating needs as well as the risk mitigation measures in place to protect the regulated private data. This includes the collection, storage and transmission of these data by third party service providers.

Unapproved collection, storage, and/or transmission of regulated private data are not permissible. Existing records containing regulated private data for which approval of collection, storage and/or transmission is not granted must be destroyed. A method that overwrites the data must be used for the deletion of such electronic records. Paper copies and reports containing such data must also be destroyed by shredding. If shredding is to be performed outside the holding office, then a signed statement attesting to the protective measures and ultimate destruction of the records must be provided to the department and retained for audit purposes.

[1] New York State defines "private information" in the *NYS Security and Breach Notification Act of 2005* as the following: bank credit/debit card account numbers with PINs, Social Security Numbers, drivers' license numbers and state-issued non-drivers' identification numbers. Since the Payment Card Industry Standard and Health Insurance Portability and Accountability Act cover credit/debit card numbers and protected health information (PHI) respectively, we add credit/debit card numbers (sans PINs) and PHI to the NY State list of "private information" items. Finally, we add passwords and computer access protection data to form our list of regulated private data.

THIRD PARTY AGREEMENTS

University at Buffalo engages in business where University data are being collected, transmitted, or stored under contracted third party arrangements. In order to minimize the risk of disclosure of University data, vendors engaged in such contracts must respond in writing to the University at Buffalo Application Service Provider IT Security and Service Criteria with detailed technical responses. The University at Buffalo Information Security Officer (ISO) will closely review the Vendor's responses and suggest remediation measures if needed. The ISO must approve a Vendor as an application service or hosted solutions provider before entering into a contractual agreement. Vendors must follow and comply with the *Standards for Securing Regulated Private Data*.

INFORMATION SECURITY BREACH AND DATA EXPOSURE NOTIFICATION

Any suspected or confirmed exposure of regulated private data or security breach of a system containing such protected data must be reported immediately to the Information Security Officer sec-office@buffalo.edu. The University at Buffalo complies with the New York State Information Security Breach and Notification Act.

COMPLIANCE AND REVIEW

The Information Security Officer will conduct annual security reviews of approved systems storing and handling regulated private data. Periodic scans of workstations, servers, and network traffic for regulated private data may also be implemented. Any employee or student who breaches the confidentiality of regulated private data will be subject to disciplinary action and/or sanctions up to and including discharge and dismissal in accordance with University policy and procedures.

APPLICABILITY

This policy applies to all University entities, any official or administrator with responsibilities for managing regulated private data, and those employees who are entrusted with regulated private data. Sub-section

Contact Information

Information Security Officer
517 Capen Hall
University at Buffalo
sec-office@buffalo.edu
(716) 645-8126

Related Information

University Documents:

Standards for Securing Regulated Private Data
Application Service Provider IT Security and Service Criteria (available on request from the Information Security Office)
Information Security: Data Access and Security Policy
Social Security Number Policy

Other Documents:

New York State Information Security Policy

Presidential Approval

Signed by President John B. Simpson 1/9/2009

John B. Simpson, President **Date**