Title: Data Breach Notification Policy Policy: 6610

Purpose

This Data Breach Notification policy reflects the University's commitment to protect data confidentiality and integrity surrounding its Information Technology (IT) systems and data. The University has implemented business processes to adequately respond to a data breach of personal identifiable information (PII) or medical information maintained on its systems and/or on the University campus.

Authority, Responsibility, and Duties

The IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Refer to Information Security Policy 6110 for roles and responsibilities.

Chief Information Security Officer (CISO)

The VSU CISO is responsible for managing the Data Breach Notification process and keeping University stakeholders (i.e., VSU President, Vice Presidents, IT Management, etc.) informed. The CISO will provide notification that consists of:

a. A general description of what occurred and when;
b. The type of Personal Information that was involved;
c. What actions have been taken to protect the individual's Personal Information from further unauthorized access;
d. A telephone number that the person may call for further information and assistance, if one exists; and
e. What actions the University recommends that the individual can take. The actions recommended should include monitoring their credit report and reviewing their account statements (i.e., credit report, medical insurance Explanation of Benefits (EOB), etc.).

Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

Policy Statements

1. Identify and document all University systems, processes, and logical or physical data storage locations (whether held by the University or a third party) that contain personal information or medical information.

    a. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

        1) Social security number;
        2) Driver's license number or state identification card number issued in lieu of a driver's license number; or
        3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;

    b. Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

        1) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
        2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

2. "Redact" for personal information means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

    a. Five digits of a social security number; or
    b. The last four digits of a driver's license number, state identification card number, or account number.

3. "Redact" for medical information means alteration or truncation of data such that no information regarding the following are accessible as part of the medical information:

    a. An individual's medical history; or
    b. Mental or physical condition; or
    c. Medical treatment or diagnosis; or
    d. No more than four digits of a health insurance policy number, subscriber number;
    e. Other unique identifier.

4. Include provisions in any third party contracts requiring that the third party and third party subcontractors:

    a. Provide immediate notification to the University of suspected breaches;
    b. Allow the University to both participate in the investigation of incidents and exercise control over decisions regarding external reporting; and
    c. Assume financial responsibility for the cost of breach notification in the event they are responsible for the breach.

5. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information or medical information by any mechanism, including, but not limited to:

    a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
    b. Theft or loss of physical hardcopy; and
    c. Security compromise of any system containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.).

6. An individual or the University shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

7. If a Data Custodian is involved in the data breach, they must alert the Data Owner and CISO.

8. The CISO shall provide this notice to those individuals affected without undue delay, as soon as, verification of the unauthorized release is confirmed, except as delineated in #9,

below. Provide this notification by one or more of the following methodologies, listed in order of preference:

a. Written notice to the last known postal address in the records of VSU;
b. Telephone notice;
c. Electronic notice; or
d. Substitute notice - if VSU demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or VSU does not have sufficient contact information or legal consent to provide notice.

Substitute notice consists of all of the following:

i. Email notice if VSU has email addresses for the members of the affected class of residents;
ii. Conspicuous posting of the notice on the web site of VSU; and
iii. Notice to major statewide media.

9. Hold the release of notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law enforcement agency determines and advises VSU that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

11. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules. The VSU CISO shall notify the CISO of the Commonwealth when notification of affected individuals has been completed.

References

Virginia Department of Human Resources Management:

Policy 1.60 Standards of Conduct (4/16/08, 6/1/11)
Policy 1.75 Uses of Electronic Communication and Social Media (8/01/01, 3/17/11)

Virginia Information Technology Agency (VITA):

Information Security Standards (SEC501-07) (1/28/2013)
IT Security Audit Standard (SEC502-02) (12/05/2011)
IT Systems Security Guideline (SEC515-00) (07/17/2008)

Title: Data Breach Notification Policy Policy: 6610

NIST Special Publications

Recommend Security Controls for Federal Information Systems and Organizations SP 800-53

Approval By: _____ 5/10/18

President

Date: _____