Purpose

The Data Breach Policy specifies the notification requirements that will be used by Virginia State University (VSU) to identify triggering factors and necessary responses to unauthorized release of unencrypted sensitive information.

Policy Statement

This policy applies to all University employees, students, business partners, and contractors who use VSU information technology resources to conduct University business and to transmit sensitive data in the performance of their jobs.

Authority, Responsibility, and Duties

The Virginia Information Technology Agency (VITA) Information Security Standard (ITRM Policy SEC 501-01) requires the University to establish a baseline for IT security controls, which will allow the University to accomplish its mission in a safe and secure environment. In respect to data breach notification:

A. The Office of Information Technology (OIT) is required to:

1. Identify all University systems, processes, and logical and physical data storage locations (whether held by the University or a third party) that contain Personally Identifiable Information (PII) such as social security number, drivers license or identification card number, financial account number, credit or debit card number, or other personal identifying information, such as insurance data or date of birth.

2. Include provisions in any third party contracts requiring that the third party and third party subcontractors provide immediate notification to the University of suspected breaches, and allow the agency both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.

3. Provide appropriate notice to affected individuals upon the unauthorized release of any unencrypted PII by any mechanism, including, but not limited to:

   a. Theft or loss of digital media including laptops, desktops, tablets, CD’s, DVD’s, tapes, etc.;

   b. Theft or loss of physical hardcopy; or

   c. Security compromise of any system containing PII.

Revision Date:   Page No: 1
4. Provide this notice without undue delay as soon as verification of the unauthorized release is confirmed unless it would interfere with ongoing data breach investigation or investigation of root cause with Law Enforcement entities or Chief Information Security Officer (CISO).

5. Provide notification that consists of:
   a. A general description of what occurred and when;
   b. The type of PII that was involved;
   c. What actions have been taken to protect the individual’s personal information from further unauthorized disclosure;
   d. What will the University do to assist affected individuals, including contact information for more information and assistance; and
   e. What actions the University recommends that the individual take when a breach occurs.

6. Provide this notification by one or more of the following methodologies, listed in order of preference:
   a. Standard mailing to any affected individuals whose mailing addresses are available.
   b. Electronic mail to any affected individuals whose email address has been provided to the University as a contact mechanism.
   c. In the case of large scale breaches or data breaches where neither form of communication listed above is available or feasible, public communications channels, including University website and/or notification by statewide public media such as newspapers, radio, and television.

7. Establish an IT Security Incident Handling process for reporting data breaches and IT security incidents to the CISO in accordance with Code of Virginia 2.2-603(F).

B. The Department of Police and Public Safety (DPPS) is required to notify the Information Security Officer (ISO) of lost and/or stolen IT computers or equipment including laptops and hand held devices.

C. All VSU employees, students, and contractors are required to notify the ISO if they suspect or are aware of data breaches related of lost and/or stolen IT computers or equipment including laptops and hand held devices. It is also the responsibility of all VSU employees, students, and contractors to notify the ISO if they have PII stored on desktops, laptops, digital media, and mobile devices including external hard drives. OIT will retrieve the device containing the PII and exchange for a new device.
Definitions

Personally Identifiable Information (PII) is any piece of information that can potentially be used to uniquely identify, contact, or locate a single person.

Information Security Officer (ISO) is responsible for overseeing the implementation of the University’s Information Technology (IT) Security program.

Information Technology (IT) Security Breach is the violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Incident is an adverse event or situation, whether intentional or accidental that poses a threat to integrity, availability, or confidentiality of an IT system.

References

Virginia Information Technology Agency (VITA):
Information Technology Security Standard (ITRM Standard SEC501-01)

Virginia State University (VSU):
Policy 6520: Acceptable Use Policy
Policy 6420: Electronic Records and Retention Policy
Policy 6110: IT Resource Security Policy
Policy 6640: Network Monitoring Policy
Policy 6530: Security Awareness Training Policy
Policy 6310: Banner Security Policy
Policy 6620: IT Security Handling Policy

APPROVED BY: [Signature]
President
Date: 4/23/08

Revision Date: Page No: 3