Procedures to Accompany the UNLV Breach of Information Notification Policy

Introduction

UNLV has a responsibility to protect the personal, sensitive information of the many constituents it serves (e.g., students, faculty, staff, donors, alumni, etc.). Despite best efforts to secure the information, occasionally, a breach may still occur. The procedures below are designed to provide an immediate response to any suspected breach. They ensure that the affected individuals are notified as quickly as possible while keeping the university compliant with federal and state regulations as well as with NSHE policies and the UNLV Breach of Information Notification.

Step 1: Report Suspected Breach

Any member of the campus community or any campus constituent (e.g., alumni, member of any NSHE institution) who suspects or discovers a data breach must report the breach. Reports should be submitted via email to breachreport@unlv.edu. The subject line should contain the words "suspected breach."

Additionally, the email regarding the suspected breach should include as much of the following information as possible:

1. Reason for suspecting a breach
2. Type of information breached, if known
3. Date or period of time breach occurred, if known
4. Contact information of person reporting the breach including phone number
5. Any other relevant information

All reports of suspected breaches will be kept confidential.

Step 2: Investigate Suspected Breach

The Information Security Office will investigate every suspected breach that is reported. In the case of electronic records, a complete forensic analysis of the affected systems will be done to determine if an actual breach occurred and, if so, the extent of that breach.

If it is determined that a breach occurred, notification of the affected individuals will be done by one of two processes.

<u>Expedited Notification</u>
The "expedited" notification process is used only for very small (<25 individuals) breaches. In this process, the Information Security Office handles all remaining steps of the breach procedures and no breach response team is formed (Step 3 of the procedures are omitted). In circumstances where the breach is limited only to the user of the compromised system, the Vice Chancellor for Information will not be notified.

Full Notification

The “full” notification process follows the procedures outlined in the remainder of this document. It should be noted that in certain circumstances, a breach that would normally be “expedited” may be elevated to the “full” process. This is done at the discretion of the Vice Provost for Information Technology.

The following matrix shows when a breach is classified as either an “expedited” or a “full” process.

Breach Classification Matrix							
			Data Type				
		Age of Access	**SSN**	**Credit Card #**	**FERPA**	**HIPAA**	**Letter**
Size	**User**	New, Old, Very Old	Expedite	Expedite	Expedite	Expedite	L1
	Small < 25	New < 2 years	Expedite	Expedite	Expedite	Expedite	L2
		Old 2-4 years	Expedite	Expedite	Expedite	Expedite	L3
		Very Old 4+ years	Expedite	Expedite	Expedite	Expedite	L4
	Medium 25 to 100	New < 2 years	Full	Full	Full	Full	L2
		Old 2-4 years	Full	Full	Full	Full	L3
		Very Old 4+ years	Full	Full	Full	Full	L4
	Large >100	New < 2 years	Full	Full	Full	Full	L2
		Old 2-4 years	Full	Full	Full	Full	L3
		Very Old 4+ years	Full	Full	Full	Full	L4

Step 3: Form Response Team

Upon determination that the breach is classified as a “full” breach, the Vice Provost for Information Technology or designee will form the appropriate Breach Response Team.

The Breach Response Team will consist of the following members to be determined by the nature of the breach:

- Vice Provost for Information Technology
- Appropriate Cabinet Level Executive(s)
- General Counsel
- Director of Media Relations
- Appropriate Data Steward
- Appropriate member(s) of the unit in which the suspected breach occurred
- Member of Information Security Office
- Other members as determined by the Response Team

If student data is involved in the suspected breach, the Breach Response Team will also include:

- UNLV Registrar
- Executive Director of Financial Aid and Scholarships

The Breach Response Team will:

- Review all information relevant to the breach
- Request additional information from appropriate sources as needed
- Determine the impact of the breach
- Assist in the containment of the breach, if necessary
- Prepare a Breach Response Plan

Step 4: Create and Implement a Breach Response Plan

The Breach Response Plan must include:

- Notification of those affected by the breach by the unit in which the breach occurred
- Create appropriate general disclosure communications
- Time frames for completing each portion of the plan
- Assignments of the parties responsible for completing each portion of the plan
- Any other information that will ensure that the breach is contained and those affected are notified in a timely manner

Step 5: Close Breach Incident

After notification is complete the Information Security Office must, in accordance with NSHE policy, submit a completed *NSHE Data Breach Notification Form* to the Vice Chancellor for Information Technology and the System Security Officer. Submission of this form constitutes the close of the breach incident.

In breach incidents that involve student data, a copy of the *NSHE Data Breach Notification Form* will also be sent to the UNLV Registrar and the UNLV Executive Director of Financial Aid and Scholarships. These offices will submit reports for their areas in accordance with federal regulations, if necessary.

All records related to breach incidents will be retained by the Information Security Office for a minimum of two years from the close of the incident. These records may be used to:

- Respond to requests as required by federal and state laws, and NSHE regulations and/or policies
- Assist with the assessment of campus information security measures

At the end of the retention period all records will be disposed of securely.

Definitions

Breach - Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of sensitive, personal information maintained by the university or its employees. Good faith, but unauthorized, acquisition of such sensitive, personal information by an employee or agent of UNLV for university business is not a breach for purposes of this policy, provided that the information is not subject to further unauthorized disclosure.

Disclosure - Notification using one of the following methods:

(1) Notice in writing either hand delivered or mailed to the address on file with, or last known to, the university

(2) Notice by email if the individual has an email address on file with the university

Sensitive, personal information - Any information about the individual maintained by the university, including the following: (a) Education, financial transactions, medical history, and criminal or employment history; and, (b) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. [38 USCS § 5727(19)]

Sensitive, personal information does not include publicly available directory information that may be lawfully disclosed.