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 NSHE policies and the UNLV Breach of Information Notification Policy.

Step 1: Report Suspected Breach

Any member of the campus community or any campus constituent (e.g., alum, member of 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 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, the NSHE Chief Information Security Officer (CISO) will be notified within 24 hours of the unit's or institution's discovery of any such breach using the form shown in Appendix A.

Notification of the affected individuals will be done by one of two processes.

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 NSHE Chief Information Security Officer (CISO) will not be notified.

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.

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

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 Custodian
- Appropriate member(s) of the unit in which the suspected breach occurred
- Member of the Information Security Office

- Other members as determined by the Response Team

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, if necessary, in the containment of the breach
- 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
- 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 will complete the *UNLV Breach Incident Closure Form* shown in Appendix B. Completion of this form constitutes the close of the breach incident.

In breach incidents that involve student data, a copy of the *UNLV Breach Incident Closure Form* will also be sent to the appropriate data custodian. The data custodian will submit reports, if necessary, in accordance with federal regulations.

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.

Appendix A - NSHE Data Breach Initial Notification Form

NSHE Data Breach Initial Notification Form

Please use the drop-down or enter text as appropriate below. When completed, please save the file as "Data Breach Notification - <your institution>" and send to NSHE CIO for Information Technology, Anne Milkovich at amilkovich@nshe.nevada.edu and cc: Chief Information Security Officer Theresa Semmens at tsemmens@nshe.nevada.edu.

Institution:

Date Breach Occurred:

Date Breach Identified:

Departments Affected:

Type of Data Exposed (e.g. *SSN, Credit Card #, Student ID*):

Number of Records (*if known*):

Is Breach internal or external?

Which federal, state and/or industry regulations does the breach affect?

If required, will notification be provided to regulatory agencies?

What is the current phase of the incident response process, e.g., Identification, Detection, Containment, Remediation, Recovery?

Is there a possibility of a criminal nature involved in the breach?

Contact if further information required:
Name:
Phone:
E-mail:

Please do not send personally identifiable information, including screen shots, via e-mail.

Appendix B – UNLV Breach Incident Closure Form

UNLV

UNLV Breach Incident Closure Form

Please fill in the appropriate information below. This form will be sent to the appropriate data custodian and a copy will be retained by the Information Security Office.

Date Breach Occurred:

Date Breach Identified:

Departments Affected:

Type of Data Exposed (e.g. *SSN, Credit Card #, Student ID*):

Number of Records (*if known*):

Was Breach internal or external?

Which federal, state and/or industry regulations does the breach affect?

Have all parties been notified as required?

What was the method of notification?

On what date was the notification completed?

Contact information of the person completing this form:
Name:
Phone:
E-mail:

Please do not send personally identifiable information, including screen shots, via e-mail.