UNLV

OFFICE OF INFORMATION TECHNOLOGY

BREACH OF INFORMATION NOTIFICATION POLICY

RESPONSIBLE ADMINISTRATOR: VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(S): OFFICE OF THE VICE PROVOST FOR INFORMATION TECHNOLOGY
ORIGINALLY ISSUED: MAY 10, 2007
APPROVALS:

APPROVED BY:

Lori L. Temple, Vice Provost for Information Technology — *Date* 04/9/15

APPROVED BY:

John Valery White, Executive Vice President & Provost — *Date* 4/2/15

APPROVED BY THE PRESIDENT:

Len Jessup — *Date* 4-27-15

REVISION DATE: APRIL 2015

STATEMENT OF PURPOSE

The purpose of this policy is to ensure that the university meets its disclosure obligation in the event of an inappropriate release of sensitive, personal information.

ENTITIES AFFECTED BY THIS POLICY

Entities affected by this policy include UNLV students and employees and anyone interacting with UNLV.

WHO SHOULD READ THIS POLICY

UNLV students and employees and anyone engaging in business with UNLV should read this policy.

POLICY

The university shall disclose any breach of its data to any person whose sensitive, personal information was, or is reasonably believed to have been, acquired by an unauthorized person. This disclosure shall be made in the most expedient time possible. It is the university's sole discretion to determine the scope of the breach.

The disclosure may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

The university shall make every reasonable effort to contact individuals impacted. Contact may be made in person, by mail, and/or by e-mail.

If the university does not have sufficient contact information, a general disclosure will be posted on a UNLV web site and appropriate news media outlets will be notified.

The university will provide information about data breaches as required by federal and state laws, and NSHE regulations and/or policies.

For additional information, including how to request an exception to this policy, refer to the Office of Information Technology's Policies and Procedures web page at http://oit.unlv.edu/about-oit/policies.

RELATED DOCUMENTS

Nevada System of Higher Education (NSHE) Regents Handbook, Title 4, Chapter 1, Section 22, 7(a), (B/R 06/13), Information Security Policy http://system.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Handbook/T4CH01GeneralPolicyStatements%281%29.pdf

NSHE Procedures and Guidelines Manual, Chapter 14, Section 1(3) & (4)4 (B/R 03/13, Data and Information Security) http://system.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Procedures/PGMCH14DATAANDINFORMATIONSECURITY(1).pdf

NRS 603A – Security of Personal Information - http://www.leg.state.nv.us/NRS/NRS-603A.html

CONTACTS

Refer to the Office of Information Technology's Policies and Procedures web page at http://oit.unlv.edu/about-oit/policies for the procedures associated with this policy and a list of individuals who can answer questions about the policy.

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 e-mail if the individual has an e-mail address on file with the university

Every reasonable effort – Use all contact information available in university records to notify individuals who may have been impacted**.**

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.