




OFFICE OF INFORMATION TECHNOLOGY

DATA CONFIDENTIALITY POLICY FOR CONTRACTORS

RESPONSIBLE ADMINISTRATOR: VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(S): OFFICE OF THE VICE PROVOST FOR INFORMATION TECHNOLOGY
ORIGINALLY ISSUED: JULY 2015

APPROVALS:

APPROVED BY:

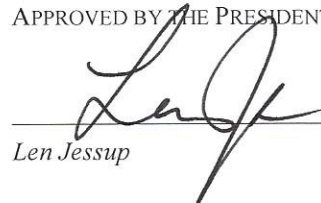


Lori L. Temple, Vice Provost for Information Technology 07/20/15
Date



Nancy Rapoport, Executive Vice President & Provost 7/21/15
Date

APPROVED BY THE PRESIDENT:



Len Jessup 8-4-15
Date

REVISION DATE: NA

STATEMENT OF PURPOSE

The purpose of this policy is to:

- Ensure employees understand their responsibilities when they contract with individuals or companies or who may have access to campus data during their engagement with the university.
- Ensure contractors understand their responsibilities for the protection of data during the performance of their contracted services.
- Ensure contractors who access data, directly or indirectly, are in compliance with all applicable laws and regulations, as well as relevant UNLV policies and procedures.

ENTITIES AFFECTED BY THIS POLICY

Entities affected by this policy include parties that enter into contracts with UNLV and UNLV representative(s) responsible for those contracts.

WHO SHOULD READ THIS POLICY

UNLV employees who develop, manage, oversee, and/or execute contracts should read this policy. Additionally, any individual or company contracted by UNLV should read this policy.

POLICY

Contractors who receive or are provided access to university data will use the data solely for the purposes for which they have been contracted. Contractors who are exposed to protected information during the scope of services will use and disclose protected information solely and exclusively for the purposes for which such information, or access to it, is provided in order to perform services. Contractors are fully responsible and liable for all acts, omissions, and work performed by their representatives or subcontractors.

Contractors hired through the UNLV procurement process are bound by the terms and conditions associated with the protection of university data included in the executed contract.

Contractors hired to work specifically with Protected Health Information must complete a HIPAA Business Associate Agreement.

All other contractors must comply with all provisions of the Contractor Confidentiality Agreement. The agreement can be modified with approval of General Counsel.

Employees are responsible for ensuring contractors who receive or are provided access to university data comply with their responsibilities as set forth in this policy.

Refer to the Office of Information Technology’s Policies and Procedures web page at <http://oit.unlv.edu/about-oit/policies> for additional information and exceptions.

RELATED DOCUMENTS

Contractor Confidentiality Agreement (link to be added when document is ready)

UNLV Data Governance Policy - https://www.unlv.edu/sites/default/files/page_files/27/Policies-DataPolicy.pdf

Nevada Revised Statute Chapter 603A - Security of Personal Information - <http://www.leg.state.nv.us/NRS/NRS-603A.html>

HIPAA Business Associate Agreement - To obtain this document work with the appropriate UNLV HIPAA unit. For a list of UNLV HIPAA units refer to the Office of Information Technology’s Policies and Procedures web page at <http://oit.unlv.edu/about-oit/policies>

Procurement Process Information - Contact UNLV Purchasing for questions about the terms and conditions associated with the protection of university data included in contracts.

CONTACTS

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

DEFINITIONS

Contractor - An individual or company that is under agreement (i.e., hired or engaged in any way) to provide services to UNLV or engages with UNLV in a vendor demonstration that includes access to university data as part of the demonstration.

Data - The observations and information collected or accessed during the performance of services, including protected information and images with a reasonable expectation of privacy.

Protected Health Information – Has the meaning set forth in the Health Insurance Portability and Accountability Act of 1996 and any subsequent amendments (HIPAA, codified at 42 U.S.C. 1320(d); Protected data definition at 45 C.F.R. § 160.103).

Protected information - Information provided at the direction of UNLV or to which access was indirectly obtained in the course of contractor's performance of services, that:

- is an education record, protected health information, or personally identifiable information;
- identifies any individual (by name, signature, address, telephone number, email address, or other unique identifier);
- can be used to authenticate any individual (including, but not limited to, any employee identification number, Social Security number, driver's license number or other government-issued identification number, passwords or PINs, biometric or health data, answers to security questions, or other personal identifiers); or, includes credit card, debit card, or other financial information.

UNLV business contact information is not, by itself, protected information.
