Campus Data Security Policy

Issued: September, 2009
Responsible Official: Director of IT
Responsible Office: IT Central

POLICIES

Policy Statement

Policy

In the course of its operations, Minot State University (MSU) collects and maintains restricted data about students, employees, donors, vendors, and others. This policy governs the use, control, and access to restricted data defined by statute, regulation, contract, license, or definitions within this policy.

University data must be protected against threats such as malicious misuse, unauthorized intrusions, and/or inadvertent compromise. Each MSU department and employee is responsible for the integrity and security of University data used, controlled, or accessed within their area. This policy establishes parameters for protection of University data, not the medium or application that the data resides in. This policy aligns with other established policies and procedures for data security and NDUS Procedure 1901.2 Computer and Network Use.

Prior to use of restricted University data via laptop computer or other electronic portable data device, employees are responsible for obtaining appropriate protections for such computers or portable devices, or for verifying that such protections are already in place. The use of unprotected equipment to access or store University data is prohibited, whether or not the equipment is owned or controlled by the University.

Responsibilities

The Director of Information Technology (IT) is responsible for implementing appropriate data security policies, procedures, and technology standards (i.e. hardware and software) for the University.

MSU employees are responsible for protecting restricted University data to which they have access. Data security standards and procedures are posted at http://www.minotstateu.edu/itcentral/policies.shtml. Department heads are responsible for insuring their employees have knowledge of and access to MSU data security standards and

procedures. This responsibility extends to data accessed on University office equipment, as well as personally owned equipment on which restricted University data is stored or manipulated.

Purpose

The Minot State University is committed to maintaining the confidentiality of all restricted University data. The purpose of this policy is to establish classifications for University data and a framework to preserve the integrity of all University data, regardless of the hardware, systems, etc. where the data may reside in or be accessed from.

Definitions

Data Steward	University officials and agents of the University who have designated duties for collection, input, and maintenance responsibilities for data within their functional area.
Encryption	Programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key. Transforming information using a secret key so that the information is unintelligible to unauthorized parties.
ERP System	Any centralized data storage or distribution system on campus. Enterprise Information Systems are managed by ITD.
Internal/Limited Access University Data	Data that would not expose the University to loss if disclosed, but should be protected. Internal/limited access University data includes, but is not limited to, operational data likely to be distributed across organizational units within the University.
Network	Any number of computers and portable devices joined together by a physical or wireless communications link that allows information to be passed between computers, irrespective of where those computers are located. Networks provide the

	pathways for information traffic and allow employees to access databases and share applications residing on servers.
Personally Identifiable Information (PII)	Data that can be used to uniquely identify an individual.
Portable Devices or Media	Portable devices include laptops, Personal Digital Assistants (PDA), or any other portable technology hardware. Media includes technology storage mediums such as CDs, DVDs, magnetic tapes, floppy disks, external hard drives, and universal serial bus (USB) drives, or any other portable data storage media.
Public University Data	Data available within the University community and to the general public.
Restricted University Data	Data protected by federal or state law or regulations, or by contract. Restricted University data includes, but is not limited to, data that is protected by the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the Gramm-Leach Bliley Act (GLBA).
Server	An application or hardware that performs services for connected clients as part of a client server architecture.

Procedures

General Security	Data security procedures, technology standards, and best practices can be found at http://www.minotstateu.edu/itcentral/policies.shtml. Employees are responsible for insuring that appropriate security controls in accordance with published University standards are installed on their office and personal/home computers or any portable devices or media on which restricted University data is stored or accessed. Restricted University data must be protected against physical theft or loss, electronic invasion, or unintentional exposure through a variety of personal and technical means. All University computers must have recommended operating

system patches and updates installed, updated antivirus and antispyware tools installed, and firewalls turned on. Personal passwords are established and secured by employees. Passwords are not to be disclosed or shared.

IT Central is responsible for the security of all Enterprise Information Systems across campus including ImageNow, Active Directory, Exchange email and calendaring system, Sharepoint, and Blackboard learning management system.

IT Central will audit servers, computers, and portable devices or media with restricted data for compliance with policies and standards and will deny network access for servers, computers, and portable devices or media out of compliance.

Remote Access

Remote access to restricted University data is available only to authorized employees. Employees must be authenticated to access restricted University data remotely. Data must be encrypted during transit.

Home Computers

Home computers that are used to access, store, or transmit restricted University data should use current security patches, updated antivirus and antispyware software, and encryption. In instances where standard security precautions are not free, the employee will incur all costs for security of their home computer.

Employees are responsible for deleting all restricted University data from their computer upon termination of employment.

Portable Devices or Media

Each user in the possession of restricted University data is responsible for protecting the data, regardless of the portable devices or media the data resides on.

Restricted University data may not be loaded onto any portable device or media unless protective measures are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss. Protective measures must be implemented before restricted University data is installed.

Restricted University data stored on portable devices or media must be encrypted. The University's data encryption standard is located at http://www.minotstateu.edu/itcentral/encryption.shtml.

Equipment Disposal	University-owned computers and portable devices or media must have all confidential and official university data erased from the computer or portable device or media prior to its transfer out of University control, and/or destroyed, using University standards for inventory disposal.
Failure to Comply with this Policy	Failure to comply with current data security procedures may result in limiting or denying access to University data resources. If, upon investigation, the lack of compliance appears to have been willful and deliberate, disciplinary action may be taken. IT Central and NDUS Policies available from http://www.minotstateu.edu/itcentral/policies.shtml should be reviewed at the beginning of each academic semester by all users who have access to restricted University data.