Current Status: *Active* **PolicyStat ID:** *9777748*

Origination: *01/2015*
Last Approved: *06/2021*
Last Revised: *06/2021*
Next Review: *06/2022*
Owner: *Andrew Violet: Senior Security Analyst*
Area: *Information Technology - Security Policies*
References:
Applicability: *Des Moines University*

Assigned Security Responsibility

I. POLICY

Purpose, Scope, and Governing Policy statements can be found in the Information Security and Privacy Overview Policy.

A. The Information Security Officer is responsible for maintaining the University information security policies and is held accountable for the guidance, direction, and authority for information security activities for the entire University. The Information Security Officer must:
   a. Review the policies according to the university's review cycle and whenever significant University changes occur, and update appropriately.
   b. Ensure that information systems are regularly checked for compliance with security and privacy policies and associated implementation standards.

B. The Privacy Officer is responsible for maintaining the University privacy policies and is held accountable for the guidance, direction, and authority for privacy activities for the entire University. The Privacy Officer must:
   a. Review the policies at least annually and whenever significant University changes occur, and update appropriately.

C. The President reviews and approves the information security and privacy policies and is ultimately responsible and accountable for ensuring all personnel know, understand and follow the policies.

D. All University personnel, contracted workers, temporary workers, and students ("Covered Individuals") with access to confidential information, protected health information (PHI) and other types of personally identifiable information (PII), owned by or entrusted to the University are responsible and accountable for knowing and complying with the University information security and privacy policies and are expected to take adequate measures to protect such information in all forms including, but not limited to, the following:
   a. On all types of computers, including mobile computers and devices
   b. On networks (data and voice)
   c. On 3rd party networks that are a result of cloud based services contracted with the university.
   d. On storage media (e.g., hard drive, flash drive, DVDs/CDs, etc.)
   e. In physical storage environments (e.g., offices, filing cabinets, drawers)

f. On printed media (e.g., paper forms, reports, etc.)

E. All Covered Individuals are responsible for protecting all University information assets. Covered Individuals are responsible for following all policies and procedures and additionally are responsible for:

a. Reading, understanding and complying with this policy and all other information security and privacy policies.

b. Signing and abiding by the Information Technology Statement of Understanding and Responsibility when accessing confidential information on the University Computer/Network Systems.

c. Ensuring all activities performed with their User IDs are in compliance with the University policies and procedures.

d. Safeguarding the University computer systems and resources from theft, destruction, unauthorized alteration or exposure, or any form of compromise resulting from inappropriate acts.

e. Maintaining the confidentiality of information stored on computer resources in accordance with the applicable information security policies.

f. Ensuring they DO NOT:

- Damage or misuse any University computer system.
- Write, produce, generate, copy, propagate or attempt to introduce any computer code (i.e. virus, worm, Trojan Horse) designed to self-replicate, damage or otherwise hinder the performance of any computer's memory, file system or software. If a virus is suspected to have infected a PC, it must be immediately reported to the IT Help Desk.
- Use the University computer systems and applications to engage in any activity that is illegal under local, state or federal law. Such activities include, but are not limited to, intimidating, threatening or harassing others.
- Use the University computer systems in a manner that is unauthorized or contrary to the best interests of the University.
- Attempt to intercept any network communication for purposes including, but not limited to, reading message/file content, searching for passwords, rerouting packets or packet "sniffing".
- Access, alter or copy files of another user without prior written consent from the file owner unless management review is warranted.
- Install personally owned software or hardware on the University computer equipment, or personally owned computing equipment used for business activities or to access the University information, without prior approval from the Information Security Officer. Incompatible software or hardware can cause damage to the system and/or impact network performance.
- Violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University.
- Circumvent user authentication or security of any computer system host, network or account (hacking, social engineering and similar activities).
- Reconfigure any controls or parameters, except as authorized by the Information Security Officer.
- Acquire, possess, trade or use hardware or software tools that could be employed to evaluate or

compromise computer systems security.

- Monopolize the University computer systems, overload the network with excessive data or waste computer time, disk space, printer paper, manuals or other resources.
- Make changes to cloud application services that may compromise the security of the connection or confidential data stored within the system.

g. Controlling access to computer equipment, business technologies, confidential information, and protected health information (PHI) and other types of personal information to only those individuals whose job responsibilities require such access.

h. Securing confidential information, and protected health information (PHI) and other types of personal information, appropriately based upon risk.

i. Protecting all authorization codes and mechanism(s) such as passwords from disclosure and/or unauthorized use. Each individual is accountable for all actions performed under the assigned computer accounts.

j. Limiting the use of University's computer systems to only authorized activities.

k. Never installing unauthorized software or computer peripherals without the authorization of the Information Security Officer.

l. Making and storing backup data in safe, secure locations.

m. Immediately reporting known or suspected security weaknesses or violations to the University Information Security Officer or ITS Service Desk.

n. Returning all information and computing assets upon separation from the University.

o. Ensuring that all systems (internal or external) are designed and implemented in a way that adheres to the University's information security policies.

p. Restricting access to confidential information and PII to only those individuals who are authorized and have a business need-to-know.

q. Ensuring that access to applications, information, and information technology resources is appropriate and authorized.

r. Clearly identifying and maintaining an inventory of all information assets used for business purposes.

s. Assigning ownership for all information and assets associated with information processing.

t. Establishing rules for the acceptable use of information and assets associated with information processing facilities.

F. The University's management is responsible for:

a. Designating those Covered Individuals who require a network account by submitting a request to the ITS Service Desk. For those employees who access the network, a signed Information Technology Statement of Understanding and Responsibility must also be submitted to Human Resources. For those contractors who access the network, a signed Information Technology Statement of Understanding and Responsibility or Non-Disclosure Agreement must also be submitted to ITS (unless covered within a contractual agreement). For those students who access the network, a signed Information Technology Statement of Understanding and Responsibility will be submitted electronically at student orientation.

b. Ensuring that Covered Individuals received information security and privacy training and ongoing

awareness communications in compliance with the Awareness and Training Policy.

c. Monitoring Covered Individuals' use of the University computer systems through observation and as required by the Information System Activity Review Policy.

d. Pursuing disciplinary actions as needed in accordance with the Sanction Policy.

G. The University's approach to managing information security and its implementation (including such things as control objectives, controls, policies, processes, and procedures for information security) will be reviewed independently at planned intervals and when significant changes to the security implementation occur.

H. The University information security and privacy policies and procedures do not preempt any existing or similar laws or policies.

Related Procedures and Forms:

- Information Security and Privacy Overview Policy
- Awareness and Training Policy
- Sanction Policy
- Information System Activity Review Policy
- Information Technology Statement of Understanding and Responsibility

Approved By:

Angela Franklin, Ph.D., President

Attachments

No Attachments

Approval Signatures

Approver	Date
Angela Franklin: President	06/2021
Carolyn Weaver: Chief Information Officer	06/2021
Keith Grey: Associate Chief Information Officer	05/2021
Andrew Violet: Senior Security Analyst	05/2021

Applicability

Des Moines University