11:01:05:00 Cyber Incident Reporting and Response Policy

Purpose:

Dyersburg State Community College is committed to protecting the information and information technology assets of the college. This policy governs the actions required for reporting and responding to cyber security incidents involving DSCC information and/or information technology resources to ensure prompt and effective reporting and handling of such events.

Scope:

This policy applies to all DSCC faculty, staff and students as well as any contractors with access to any DSCC information system or data. It applies to any computing devices owned by the College that might experience a cyber security incident or data breach. It also applies to any computing device regardless of ownership, which is used to access or store restricted or confidential College data which if lost, stolen, or compromised, could lead to the unauthorized disclosure of confidential or sensitive College data including personally identifiable information (PII) for any DSCC constituent.

Policy:

1) Incident Reporting
a) Any person discovering a suspected or known cyber security incident not involving a data breach is to notify the Vice President for Technology or another IT staff member as soon as possible. This includes an observed or suspected security weakness in the college's systems or services.
b) Any suspected or known data breaches are to be reported to the Vice President for Technology immediately. If the Vice President can't be reached, the following are to be called until one of them is reached:
i) Director of Computer Services
ii) Vice President for Finance and Administrative Services
iii) Vice President for the College
iv) Vice President for Institutional Advancement and Continuing Education
v) President
c) Examples of situations to report include but are not limited to the following:
i) Ineffective security control
ii) Observed or suspected information security weakness

iii) Breach of information integrity, confidentiality or availability expectations
iv) Human errors related to information security
v) Non-compliance with information security policies
vi) Breaches of physical security arrangements
vii) Uncontrolled system changes
viii) Unexplainable malfunctions of software or hardware
ix) Access violations to computer systems
x) Web site defacement
xi) Other unusual system behavior which may be an indicator of a security attack or actual security breach

2) Incident Response

Upon the report of a suspected or known cyber security incident, the Cyber Incident Response Plan (CIRP) will be consulted for handling of the incident according to the type and severity of the incident. The CIRP will define an Incident Response Team and outline the responsibilities of that team.

The Vice President for Technology has the authority to direct the Incident Response Team to confiscate or disconnect equipment and to monitor suspicious activity as needed in the incident response process. The President will provide this direction in the absence of the Vice President for Technology.

3) Communications

All individuals involved in the reporting of or in the response to a cyber security incident should maintain confidentiality about the situation at all times. The Director of Public Information will coordinate all public releases of information about any incidents at the direction of the President. The CIRP will assist in defining appropriate communication methods and protocols.

4) Incident Response Plan Maintenance

The Vice President for Technology is responsible for maintaining the Cyber Incident Response Plan (CIRP) and periodically reviewing and updating the CIRP as needed.

Compliance:

All DSCC employees, students and contractors are expected to adhere to this policy. Failure to report known or suspected cyber security incidents or data breaches may result in disciplinary action up to and including termination of employment.

Definitions:

CIRP: Cyber Incident Response Plan which is a guide and framework to be used in the event of a cyber incident.
Cyber Incident or Cyber Security Incident: Accidental or malicious actions or events that have the potential of causing unwanted effects on the confidentiality, integrity and availability of DSCC information and IT assets.

Cyber incidents include, but are not limited to theft or loss of physical equipment, illegal access to systems or information, and failing to protect and secure electronic Personal Identifiable Information (PII) and/or Personal Health Information (PHI).

Data Breach: Unauthorized release or access of PII or other information about a student, staff or vendor not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider. Data breaches can take many forms including: hacking, lost or stolen equipment, employee negligence or policy/system failure.

FERPA: Family Education Rights and Privacy Act

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, etc. including any other personal information which is linked or linkable to an individual. This includes any information about an individual maintained by the college, including, but not limited to, education, financial transactions, medical history, and criminal or employment history.

Sensitive Data: Data that carries the risk of adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experiences by an individual whose personally identifiable information (PII) from education records was the subject of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII.

Revision History:

Written in March 2016 by the Vice President for Technology. Approved by Admin Council April 29, 2016.