Denmark College

FROM PASSIONS TO CAREERS

Information Security Policy and Procedure for handling financial data

Effective date: December 31, 2022

In accordance with GLBA under 16 C.F.R. Part 314 the institution will ensure that Federal Student Aid applicant information is protected from access by, or disclosure to, unauthorized personnel, and the institution is aware of and will comply with requirements to protect and secure data obtained from the Department of Education’s systems for the purposes of administering the Title IV programs.

For the purpose of Denmark (or its servicer’s) compliance with GLBA, “customer” information is information obtained as a result of providing a financial service to a student, past or present. Institutions or servicers provide a financial service when they, among other things, administer or aid in the administration of Title IV programs. While Denmark College does not make institutional loans, or certify or service private education loans on behalf of students, Denmark does administer Title IV programs and has therefore developed the following Information Security Policy.

The institution has designated the following individual as Information Security Coordinator responsible for overseeing, implementing, and enforcing the Information Security Program: Aaron Young, Chicago Campus Director

All student personally identifiable information (PII) is to be kept secure and accessed only by Denmark College employees and individuals who need access for work-related reasons. Student files and other documents containing sensitive information are to be maintained in locked drawers or locked offices with restricted access. All electronic transmissions must be encrypted and/or password-protected, and the password must be sent in a separate transmission.

The institution’s Information Security Program is based upon the following risk assessment to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of safeguards in place to control these risks.

Possible risks and safeguards

Risk: Access to physical student files or other documents containing PII

Safeguard: Student files are kept in locked drawers, locked cabinets, or locked offices. Keys should remain the possession of the responsible staff member.

Safeguard: Only employees with a need are allowed access to student files.

Safeguard: All student records with financial data to be disposed of are shredded.

Risk: New staff members will not be aware of the student file safeguard policy

Safeguard: New staff members with a need to access student files will be trained on the policies and procedures of the College including those related to handling of financial data.

Safeguard: Information Security Policy and Procedure for handling financial data is disseminated at least annually to all employees.

Risk: Information can be accessed on the network

Safeguard: The network is restricted to staff only.

Safeguard: Computers with access to the staff network are password-protected. Staff members are not to share passwords with others. Staff members are instructed not to leave computers unlocked and unattended.

Safeguard: Only staff members with a need are allowed access to the areas on the network where financial information is maintained.

Safeguard: Access to shared drives on the network is restricted to Denmark computers.

Risk: Information can be exposed via electronic transmission

Safeguard: Electronic transmission of student PII should be kept to a minimum. Inter-company transmission must be done via the shared drive on the secure staff network rather than via e-mail.

Safeguard: Should it be necessary to transmit via e-mail (such as in communication with third-party servicers), all student PII must be password-protected and passwords sent in a separate transmission.

Risk: Information may be vulnerable to cyber attacks/hacking

Safeguard: For detecting and preventing attacks we use ESET antivirus along with a Pfsense firewall at each location.

Safeguard: In the event of a system failure, Denmark College contacts Best Servers via help@bestserversllc.net or 219-756-5280 Opt2 for resolution.

Safeguard: Our IT service provider, Best Servers, employs real time alerts that are continually monitored to identify any system failures.

Risk: Third party servicers with access to financial data have a breach

Safeguard: Limit the number of service providers who have access to financial data to those that are necessary.

Safeguard: Perform due diligence on all service providers to ensure they maintain appropriate safeguard before doing business with them.

Safeguard: All contracts with service providers require the service providers to maintain appropriate safeguards to ensure protection of financial data.

Risk: Student Credit Card Details may be Compromised

Credit card numbers are, as a rule, not retained. Students with recurring payments are responsible for bringing in/calling in payments each time they wish to make a payment. For those requiring recurring automatic payments who do provide credit card information, this information is kept in a locked office with access restricted only to authorized personnel.

Risk: Information Security Policy and Procedures become outdated

Safeguard: Information Security Policy and Procedure for handling financial data is evaluated/updated at least annually. Additional risk assessments shall be performed periodically to reexamine reasonably foreseeable internal and external risks to security, confidentiality, and integrity of customer, and the sufficiency of any safeguards in place shall be reassessed. Current safeguards shall be regularly tested or otherwise monitored for effectiveness. This shall occur annually at minimum and a report including the following shall be presented to a senior officer of the college to include the following information:

1. The overall status of the information security program and the institution's compliance; and
2. Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's response, and recommendations for changes in the information security program, if necessary.

Any additional risks identified shall require implementation of additional safeguards to control these risks. Evaluation and adjustment of the Information Security policy shall be adjusted as necessary based upon testing and monitoring, any material changes to the institution's operation and business arrangements, the results of risk assessments, or any other circumstances that the institution knows, or has reason to know, may have a material impact upon the information security program.