|  |  |
| --- | --- |
| Information Technology Policies Manual | **Section 300.03A** |
| Policy: **Information Technology Security PLAN** |
| Adoption date: |
| Effective date: |
| **SUBJECT: SPECIFIC USE** |  |
| Reference: GLBA, FERPA | |

Pursuant to and in accordance with the Gramm-Leach-Bliley Act, the Information Technology Security plan was developed. This document summarizes the Diné College’s comprehensive written Information Technology (IT) Security Plan mandated by the Federal Trade Commission’s Safeguards Rule and the Gramm-Leach-Bliley Act (GLBA). In particular, this document describes the IT Security Plan elements pursuant to which the Institution intends to:

Ensure the security and confidentiality of covered records, and

Protect against any anticipated threats or hazards to the security of such records, and

Protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to the College’s IT consumers.

The IT Security Plan is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including Family Educational Rights and Privacy Act (FERPA).

1. Designation of Representative:

The Institution’s IT Operation Manager is designated as the IT Security officer who shall be responsible for coordinating and overseeing the IT Security Plan. The IT Security officer may designate other representatives of the institution to cover and coordinate a particular element of the IT Security Plan.

1. Scope

The IT Security Plan applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information:

1. A student or other third party provides in order to obtain a financial service from the Institution,
2. About a student or other third party resulting from any transaction with the Institution involving a financial service, or
3. Otherwise obtained about a student or other third party in connection with providing a financial service to the person.
4. Elements of the IT Security Plan
   1. Risk Identification and Assessment: The institution intends, as part of the IT Security Plan, to undertake to identify and assess external and internal risk to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the IT Security Plan, the IT Security Officer will establish procedures for identifying and assessing such risk in each relevant area of the Institution’s operation, including:
      1. Employee training and management: The IT Security Officer will coordinate with representatives in the Institution’s Human Resources and Financial Aid offices to evaluate the effectiveness of the Institution’s procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution’s current Personnel, Policies and Procedures Manual and the IT Policy.
      2. Information System and Information Processing and Disposal: The IT Security Officer will coordinate with representatives of the Institution’s Financial Aid and Business Office to assess the risks to nonpublic financial information associated with the Institution’s information system, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution’s IT Policy Section 200.02: USE OF THE DINÉ COLLEGE NETWORK AND DATA MANAGEMENT SYSTEMS POLICY. The IT Security Officer will also assess procedures for monitoring potential information security threats associated with software systems and for managing security updates for software and operating systems.
      3. Detecting, Preventing and Responding to Attacks: The IT Security Officer will coordinate with other relevant units to evaluate procedures for and methods of detecting, preventing and responding to attacks, other systems failures and network access. The IT Security Officer will evaluate the IT security policies and procedures for coordinating responses to network attacks and developing incident response teams and policies. The IT Security Officer may elect to delegate to a representative of the Department of Information Technology the responsibility for monitoring and disseminating information about known security attacks and other threats to the integrity of networks utilized by the Institution.
   2. Designing and Implementing Safeguards: The risk assessment and analysis shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The IT Security Officer will implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.
   3. Overseeing Service Providers: The IT Security Officer shall institute methods for selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they have access. In addition, the IT Security Officer will work with other designated institutional officials to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards.
5. Adjustment to IT Security Plan:

The IT Security Officer is responsible for evaluating and adjusting the IT Security Plan based on the risk identification and assessment activates undertaken pursuant to the IT Security Plan, as well as any material changes to the Institution’s operations or other circumstances that may have a material impact on the IT Security Plan.