OUTLINE OF

Sitting Bull College
GLBA Required Information Security Program

Overview: This document summarizes Sitting Bull College's (the "Institution's") comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). In particular, this document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The Program incorporates by reference the Institution's policies and procedures enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Designation of Representatives: The Institution's IT/Finance Director is designated as the Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the Institution to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees.

Scope of Program: The Program 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 (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Program:

1. Risk Identification and Assessment. The Institution intends, as part of the Program, to undertake to identify and assess external and internal risks 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 Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- *Employee training and management*. The Program 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 policies and procedures in this area, including:
    - College Employee Handbook
    - FERPA Policy

- *Information Systems and Information Processing and Disposal.* The Program Officer will coordinate with representatives of the Institution's IT Department to assess the risks to nonpublic financial information associated with the Institution's information systems, 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 current polices and procedures relating to IT policies. The Program Officer will also coordinate with the Institution's IT Department to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- *Detecting, Preventing and Responding to Attacks*. The Program Officer will coordinate with the Institution's IT Department to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the College the responsibility for monitoring and participating in the dissemination of information related to the reporting of 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 described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer will, on a regular basis, 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 Program Officer shall coordinate with those responsible for the third party service procurement activities among the IT Department and other affected departments to raise awareness of, and to 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 will have access. In addition, the Program Officer will work with

College administration to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the President or Vice President. These standards shall apply to all existing and future contracts entered into with such third party service providers.

4. Adjustments to Program. The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.

Gramm-Leach-Bliley Act
Some of the safeguards SBC has put in to place to safeguard for risks:
The college has purchased a subscription to Barracuda PhishLine. "Barracuda PhishLine uses advanced training and simulation to both measure your vulnerability to phishing emails and to teach users how to avoid becoming victims of data theft, malware, and ransomware. Your users need to be trained to easily recognize malicious emails, especially as hackers become more sophisticated and prevalent."

With PhishLine college employees can receive training videos and other information to make them more aware of malicious emails. PhishLine can also send out simulated malicious emails and record responses of employees that fall for the malicious email. These employees can be referred for further training.

All college employees have their Office 365 accounts protected with two factor authentication. This keeps unauthorized people from accessing the email and OneDrive accounts that may contain student information.
All databases or other systems that may contain student financial information is limited only to employees that have a need to access this information. All databases or other systems cannot be accessed without the proper username and password. Backups for these systems are encrypted or stored on encrypted systems with access limited only to college IT staff.

The College is protected by a firewall to limit access to College systems from off campus. Logs and traffic are periodically reviewed to look for any attempts or suspicious attempts.

Employee access to the network from off campus is protected by two factor authentication.

Access to student financial information for third parties is governed by the FERPA policy. Before any student financial information College employees verify a proper FERPA release is in effect.

As part of the onboarding process new employees review the computer acceptable use policy with the human resource director. Employees are encouraged to annually review the policy as well as referred to the policy should any questions or violations occur throughout the year.

Software and security updates for servers, workstations and software applications that have access to student financial information are installed promptly whenever possible.