



FINANCIAL MANAGEMENT
& FUND-RAISING POLICIES

FINANCIAL MANAGEMENT POLICIES

INTRODUCTION

Date: December 1988

The Sitting Bull College Financial Management Policies Manual has been developed to provide uniform guidelines for the college's financial management activities. The SBC Board of Trustees has formally adopted this manual and thus carries weight of the Board's authority and are to be fully complied with by all College Board Members, Faculty, Staff and students. In some cases, this may require change from current policies.

Structure of Manual

The Financial Management Policies Manual has been divided into sections. Each section is referenced as shown on the Table of Contents.

Each section contains the following information:

- **Policy Statement:** These define what the college is seeking to accomplish within each policy area.
- **Specific Policy Statement:** Individual statements of policy are described and numbered for ease of reference. A policy statement indicates the rule to be followed in an activity.
- **Responsibility for Compliance:** At the end of each policy, the title of each individual responsible for making sure policies is followed as listed. This assignment of responsibility means that the individuals listed will be held accountable for monitoring the financial management process to make certain that the policy is complied with.

The Financial management policies can be changed by action of the SBC Board of Trustees.

The official copy of the Financial Management polices Manual is to be retained by the Vice President of Operations and will be placed on the Colleges shared folder under policies.

Table of Contents

POLICY: FINANCIAL MANAGEMENT	4
POLICY: ACCOUNTS PAYABLE AND PURCHASING	6
POLICY: CONSTRUCTION PROCUREMENT	11
POLICY: FINANCIAL AID	13
POLICY: DISBURSEMENTS	14
POLICY: TRAVEL	15
POLICY: HUMAN RESOURCES	19
POLICY: PAYROLL	20
POLICY: ACCOUNTS RECEIVABLES AND RECEIPTING	22
POLICY: COLLECTION OF STUDENT DEBT	23
POLICY: PROPERTY (FIXED ASSETS)	25
POLICY: AUXILIARY BUSINESS POLICIES	27
POLICY: IDENTITY THEFT POLICY	28
POLICY: GRANT WRITING COMPENSATION	31
POLICY: GRAMM-LEACH-BLILEY ACT	33
POLICY: DATA CLASSIFICATION POLICY	37
POLICY: INCIDENT RESPONSE PLAN	41
POLICY: RECORDS MANAGEMENT/RETENION/BUSINESS OFFICE	45
POLICY: OUTSTANDING CHECKS POLICY	46
POLICY: INVESTMENTS	47
INTRODUCTION FUNDRAISING POLICIES & PROCEDURES	49
REGULATORY INFORMATION & LANGUAGE	49
POLICY: DONATION ACCEPTANCE POLICY	51
POLICY: DONOR PRIVACY	54
POLICY: DONOR RECOGNITION	55
POLICY: ENTERING/RECORDING DONATIONS	56
POLICY: ACKNOWLEDGING DONATIONS	57
POLICY: USE OF SITTING BULL COLLEGE NAME, LOGOS, IMAGRY, OR OTHER IDENTIFYING INFORMATION	59
POLICY: PROHIBITED ACTIVITIES	60

POLICY: FINANCIAL MANAGEMENT

Date: December 1988

Section A:

POLICY OBJECTIVES:

- To ensure and preserve the financial strength of the college through a centralized management of financial resources.
- To ensure the financial strength of the college by monitoring expenditures, budgets, and revenues collected and available cash balances.
- To provide the information required to satisfy federal standards and regulations and to meet management information needs.
- To provide support and to make the financial reporting process more useful for program directors and supervisor for compliance with all applicable federal, state, local, private and college regulations.

SPECIFIC POLICY STATEMENT

1. The Vice President of Operations and the IT/Finance Director are responsible for developing and maintaining a complete accounting system including all financial books, ledgers, records, and files to assure full accountability over college assets, commitments, and liabilities and College program revenue and expenditures.
2. The Vice President of Operations and the IT/Finance Director will review all entries to the financial books and records and monitor the recording of financial transactions to ensure complete, accurate, and timely recording and minimize possibilities for misuse or misappropriation of college assets.
3. All federal reporting requirements (including tax reporting) will be met on a timely basis. Accounting records will be maintained in a current status to facilitate reporting and to eliminate possibilities for overdrawing cash or incurring penalty and interest charges.
4. Accounting documents will be filed in a manner that permits their reconciliation to financial records monthly and that provides fully auditable support for entries made to college and program accounts. The Vice President of Operations will be responsible for the investment of college funds. The Vice President of Operations will carefully safeguard certificates or other evidence of ownership.
5. The Vice President of Operations and the IT/Finance Director are responsible for all bank accounts established to assure that revenues are deposited into the appropriate accounts and to assure that no account should be over drawn.
6. The Vice President of Operations and the IT/Finance Director are responsible for overseeing the College's certificate of deposits (CD) and have the authority to sign bank documents for issuing and renewing the College's CDs documents.
7. The IT/Finance Director will be responsible to see that each bank account is reconciled monthly to maintain control over cash flow and expenditures.
8. The IT/Finance Director will be responsible for maintaining a standard chart of accounts to provide consistency in financial reporting.
9. The Vice President of Operations will be responsible for submitting indirect cost proposals in a timely manner and in accordance with federal regulations.

10. The Vice President of Operations is responsible for the development of the annual general fund/revenue balanced budget through collaboration with supervisors on individual department needs. The annual general fund budget will be approved by the Board of Trustees prior to the start of the fiscal year of July 1.
11. The Vice President of Operations is responsible for preparing and maintaining forecasts of revenue to be collected, for assuring that revenues are collected on a timely basis, and for taking necessary steps to curtail expenditures if actual revenues do not materialize as planned.
12. The Vice President of Operations will submit a monthly financial report to the Board of Trustees to include a revenue and expenditures report, investments, bank balances, and any other information requested.
13. The Vice President of Operations is responsible for apprising department heads, supervisors, and program directors of budget control problems so that corrective action may be taken.
14. The Vice President of Operations will be responsible for initiating the process of conducting an annual audit of all college accounting records by an independent accounting firm.
15. The annual audit will be completed by March 1st for fiscal year end of June 30 as required by the federal regulations.
16. An annual audit will be submitted to the Board of Trustees for approval.
17. The financial management policies will be updated as necessary and will be distributed to all staff as required.

Responsibility:

Vice President of Operations
IT/Finance Director
President

Revised: September 2023

POLICY: ACCOUNTS PAYABLE AND PURCHASING

Date: December 1996

Section B:

POLICY AND OBJECTIVES

- To control expenditures by obtaining the lowest cost (with satisfactory quality), and by not allowing expenditures to exceed budgeting amounts.
- To make the purchasing process more efficient for Program Directors and supervisors who have the ultimate responsibility to ensure that all program purchases follow federal, state and local contract requirements as they apply and SBC policies.

SPECIFIC POLICY STATEMENTS

1. The College will follow the procurement standards as set forth in 2 CFR 200.317 to 200.327.
2. All purchases will be made only after approval of a purchase order or prior approval of President or Vice President of Operations.
3. Immediate supervisors or grant director must approve requisitions to assure budget and grant compliance and account numbers must appear on the requisition along the project account before it is presented for approval.
4. Purchases that exceed budget will be returned to originator stamped denied and reason for denial.
5. Payments will be made for specific invoices only, NOT monthly statements.
6. All original invoices should be sent directly to the Accounts Payable Technician along with adequate proof of receipt. Purchaser should sign invoice and write the appropriate PO number on the invoice.
7. Invoices submitted to the Business Office by 10 a.m. Wednesday mornings will be processed each week with checks mailed on Thursday by 3:00 p.m.
8. Purchase of any item of equipment and contractual must follow the process as outlined below: (excludes bookstore and utilities).
9. Vendors or contractors that owe the college more than \$1,000 or the debt is more than 180 days old will not be allowed to conduct business with the college until the debt is paid.

Definition: Procurement of services, supplies, or other property, with the A/E services or labor and/or materials.

<u>Price Threshold</u>	<u>Method of Procurement</u>	<u>Required Approval Level</u>
\$1 - \$500	Consumables Purchase	Sitting Bull College President or designee
\$501 to \$2,500	Micro Purchase	Sitting Bull College President or designee
\$.2501-\$25,000*	Small Purchases	\$2,501 - \$9,999 approved by the Sitting Bull College President or designee

		\$10,000 - \$25,000 must be approved by the Board of Trustees – require RFP
Over \$25,001	Large Purchases	Approved by Sitting Bull College Board of Trustees – require either IFB or RFP

Micro-purchase cannot exceed \$2,500.00

Conduct a simple price or cost analysis to determine the best value.

Small purchases \$2,501 to \$25,000.00

For items from \$2,501 to \$9,999 conduct a simple price or cost analysis to determine the best value. For items from \$10,000 to \$25,000 three (3) written prices on vendor’s letterhead or estimate forms are required to ensure you are purchasing at fair and reasonable price and must be approved by Sitting Bull College Board of Trustees prior to purchasing. Use ProcurementPro to select necessary Federal Clauses or Certifications.

Large purchases are purchases that exceed \$25,000.00

Preferred procurement methods are either Request for Proposal (RFP) or Invitation for Bid (IFB).

Request for Proposal (RFP)/Competitive Proposals

1. Develop a complete and realistic set of specifications describing in detail the professional services the procurement is requesting. Include the specific method established and used to conduct the technical evaluation of each proposal. Technical expertise and past performance considerations play a dominant role in source selection and supersede low price criteria.
2. Advertise the RFP. No geographic preferences permitted. Methods of advertising include but not limited to: newspapers, post on agency website, and send announcements letters or email to all potential bidders. The ad should include a description of the project, contact information, deadline date, how bids will be selected, and funding source. Retain proof of advertising in procurement folder. Any bids arriving after the stated date and time will be not be evaluated.
3. Formulate the evaluation team, which will review and rank all proposals received in accordance with the proposal specifications.
4. Evaluation team to evaluate and rank all proposals received using the established method and criteria. All proposals that have a reasonable chance of being selected shall be included in the Competitive range list. Review the bid against the specifications to avoid duplicative or unnecessary purchases. Verify that bidders are not on the Excluded Parties List System (EPLS) at <https://www.sam.gov> and the North Dakota and South Dakota State websites.
5. Prepare documentation and recommendation for approval from the Sitting Bull College Board of Trustees. Once approved by the Board of Trustees notification of the award will be made.

6. Monitor the contractor's progresses to determine inspection time and location. Upon completion of inspection and acceptance of products, obtain all warranty and service arrangements.
7. Finalize the payment/reimbursement vouchers.
8. Review the project file for completeness. The project file should contain all documents and written or electronic correspondence in addition, to copies of payment vouchers etc... If your procurement has multiple delivery shipments (for example rolling stock), all the documents for each delivery must be included in the original project file.

Invitation for Bids (IFB)/Sealed Bids – Required for all new Construction

1. Develop a complete and realistic set of technical specifications for the product(s) to be procured. Determine the quantity of units to be purchased plus options.
2. If a brand name product is used in the specifications to describe your needs the clause "brand name or equal" must be included after each reference to a brand name.
3. Develop evaluation process and criteria for the selection of the bid award process. In IFB the best value and responsible bidder is the most commonly used criteria.
4. Prepare your bid package, finalize the product specifications, included equals, exception, and clarification forms, official bid forms, addenda process, Disadvantaged Business Enterprise (DBE) requirements, proposal package delivery instructions, general conditions, special provisions and all Federal clauses and certifications.
5. Advertise the IFB. No geographic preferences permitted. Place ads in at least two newspapers, trade magazines, post on agency website (optional), and send announcements letters or email to all potential bidders. The ad should include a description of the project, contact information, deadline date, location of bid opening, and funding source. Retain proof of advertising in procurement folder. Any bids arriving after the stated date and time will be returned to the sender unopened.
6. Proposal Opening presentation. Complete a price or independent cost estimate, prepare bidding opening forms. Open bids, read aloud, and record all vital information. Verify that bidders are not on the Excluded Parties List System (EPLS) at <https://www.sam.gov> and the North Dakota and South Dakota State websites. Tabulate bid documents and complete selection process. Review the bid against the specifications to avoid duplicative or unnecessary purchases. Complete Pre-award audit on successful bidder. Notify selected and rejected bidders in writing.
7. Complete award selection and justification, and explain why bidder was awarded if the accepted bid was not the lowest. Confirm schedules for inspections, milestones, delivery etc., and issue and complete the contract for the procurement. Collect all documentation (completed contracts, bond, insurance etc.) and federal certifications. Issue Notice to Proceed letter.

8. Monitor vendor's progress and setup delivery and inspection time and location. Upon completion of inspection and acceptance of products, obtain all warranty and service arrangements.
9. Finalize the payment/reimbursement vouchers.
10. Review the project file for completeness. The project file should contain all documents and written or electronic correspondence in addition, to copies of payment vouchers etc... If your procurement has multiple delivery shipments (for example rolling stock), all the documents for each delivery must be included in the original project file.

Sole Source Procurement /Non- Competitive

Definition: Procurement accomplished through solicitation or acceptance of a proposal from only one available source or solicitation of a number of sources in which competition is determined inadequate.

Price Threshold	Method of Procurement	Required Approval Level
\$1 - \$9,999	Sole Source	Sitting Bull College President
\$10,000 or greater	Sole Source	Sitting Bull College Board of Trustees

Sole source procurements are accomplished through solicitation or acceptance of a proposal from only one source or after solicitation of a number of sources, competition is determined inadequate. May be used only when the award of a contract is infeasible under small purchase procedures, sealed bids, or competitive proposals and at least one of the following circumstances applies:

1. The item is available only from a single source;
2. The public exigency or emergency for the requirement will not permit a delay resulting from competitive solicitation i.e., a threat to public health, welfare, safety, property, or other substantial loss to, or a situation requiring immediate action as determined by Sitting Bull College.
3. After solicitation of a number of sources, competition is determined inadequate; or the item is an associated capital maintenance item as defined in 49 U.S.C. § 5307(a)(1) that is procured directly from the original manufacturer or supplier of the item to be replaced. The grantee must first certify in writing: (1) that such manufacturer or supplier is the only source for such item; and (2) that the price of such item is not higher than the price for such item by like customers.
4. Sole source procurements must be documented in writing and on file for review upon request explaining in detail, why this contract was issued under the Sole Source procurement method.
 - a. Equipment defined:
For Grants – any equipment with a value of \$5,000 or more. For General Fund - Any non-consumable item with a value \$5,000 or more.

SBC is subject to the non-procurement debarment and suspension regulations implementing Executive Orders 12549 and 12689, 2 CFR part 180. The regulations in 2 CFR part 180 restrict awards, sub-awards, and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in Federal assistance programs or activities. More information can be found at www.sams.gov.

The employee who is initiating the contract for a contractor, will be responsible for providing the proper documentation to ensure that the contractor is not on the debarment suspension list. The documentation must be attached to the PO or check request.

1. Consulting services will be entered into only if college staff cannot provide the required skills and must follow the purchasing requirements as statement in item number six above. The President or the Vice President of Operations must first review all consulting contracts to assure that requirements for work products and reporting are contained in the contract. See Grants Management Manual for definition of a consultant versus an employee.
2. All consultants are required to fill out a W-9 as required for issuance of 1099.
3. Payment for consulting services will be made only upon acceptance of the consultant's interim work product or report or final work product and reports. Billings must be accompanied by supporting documentation (memorandum) indicating that the services performed and cost incurred are to be paid.
4. Any consultant contract given to an employee of SBC shall be paid through the payroll process as defined in contract.

Responsibility

Vice President of Operations
IT/Finance Director
Program Directors
Accounts Payable Technician

Revised: July 2023

POLICY: CONSTRUCTION PROCUREMENT

DATE: July 2008

Section C:

POLICY AND OBJECTIVES:

- To provide guidance to administration and Board of Trustees on the process of construction bidding and construction procurement for new construction and/or renovation.
- To be able to construct new buildings and renovation projects in a cost effective manner.
- To provide a safe environment for the students, faculty and staff of Sitting Bull College.

SPECIFIC POLICY STATEMENTS:

1. Sitting Bull College will, first of all, follow all federal guidelines for procurement of grantor agency that funds any construction project.
2. Request for bids will be advertised publicly unless such project provides for sole source or special invitations to bid.
3. Bids shall be required to include any prior construction projects and completion data.
4. Bids will include a list of all required documents.
5. Bids will be opened publicly with Administration, Grant directors, architects and Board of Trustees, if required.
6. Sitting Bull College reserves the right to refuse any and all bids. Reasons for refusal will be given to the bidders.
7. Sitting Bull College has a policy for procurement/bid protest as follows:
 - a. Protest must be presented in writing to President no later than five (5) days after bid selection is announced.
 - b. The protest shall include name and address of protester; name of bid being protested; a statement for grounds for the protest with supporting documentation.
 - c. Upon receipt of protest, all activities involving the project will be placed on hold until final disposition of protest.
 - d. The president shall conduct a review of the protest within five (5) days of receipt of protest. Additional information may be requested and submitted for review.
 - e. The protestor shall be notified of the review findings and the protester will have five (5) days to respond with any additional documentation as to review findings.
 - f. The President will make a final decision within ten (10) days formally after investigating any additional materials submitted by protestor.

- g. Finally, the protestor may appeal the final findings to the Board of Trustees and in some cases, to the funding agency involved in contract within five (5) days.

Responsibility:

President

Vice President of Operations

Board of Trustees

Revise: July 2015

POLICY: FINANCIAL AID

Date: July 2001

Section D:

POLICY OBJECTIVE

- To assure proper documentation of the receipt and disbursements of Title IV federal financial aid funds.
- To assure proper documentation of all other higher education financial aid, including tribal, state and other scholarships.
- To provide for control of authorization, accountability and documentation of Title IV funds receipt and disbursement.

SPECIFIC POLICY STATEMENTS

1. The Business Office will coordinate all activity concerning Title IV funds with the college's financial aid officer
2. The Financial Aid Office will authorize all disbursements to students, payments on tuition books and fees and all refunds.
3. The IT/Finance Director will draw down all funds as authorized from Department of Education system in a timely manner with proper documentation from financial aid officer.
4. Student disbursements will be issued on a schedule authorized by financial aid office in conjunction with the IT/Finance Director.
5. No excess aid advances will be authorized.
6. Excess Title IV aid shall be paid to student in full on the first scheduled disbursement date of the semester. Any excess Title IV aid received after the initial disbursement date will be process and paid as it is received.
7. Students that have signed up for direct deposit will receive funds via ACH sent to the account of their choosing. Excess aid checks will be issued on laser checks imprinted with the signatures upon approval of IT/Finance Director. Checks will be mailed and cannot be picked up.
8. All excess aid in the amount of \$1,000 or less will be disbursed in full. If a student has excess aid below \$1,000 on the schedule disbursement date, the full amount will be released.
9. Graduate students will receive all excess aid in full during the next schedule disbursement date.

Responsibility:

Vice President of Operations
IT/Finance Director
Financial Aid Director
Accounts Payable Technician

Revised: May 2026

POLICY: DISBURSEMENTS

Date: December 1988

Section E:

POLICY OBJECTIVES

- To provide accurate and timely generation of checks (based on sound management practices) for valid, authorized expenditures.
- To include control elements necessary to properly safeguard the disbursements of the college.

SPECIFIC POLICY STATEMENTS

1. All disbursements shall be made as accounts payable checks through Sitting Bull College, records management system Jenzabar. No manual checks will be done.
2. All other one-time check, i.e. travel, salary advances, mileage or reimbursements will be due in Business Office by 10 a.m. Wednesday mornings and distributed on Thursday by 3:00 p.m. unless otherwise authorized by the IT/Finance Director.
3. No checks can be written prior to receiving approved written documents of purchase or expenditures. Example: invoices, travel reimbursements, etc.
4. If an employee makes a purchase without a purchase order and pays or charges to a personal credit card, the employee shall be responsible for the taxes paid unless they have prior approval for purchasing. Taxes are not an allowable grant cost and will need to be paid through the College's general fund.
5. No check will be processed unless the expenditure follows allowable costs following the Purchasing and Accounts Payable policies.
6. In the case of invoices not supported by the required approved purchase order, the Accounts Payable Technician will forward the invoice to the immediate supervisor of the individual who made the purchase.
7. Accounts Payable checks will be issued on laser checks with imprinted signatures upon approval by Vice President of Operations or the IT/Finance Director.

Responsibility:

Vice President of Operations
IT/Finance Director
Accounts Payable Technician
Supervisors

Revised: July 2023

POLICY: TRAVEL

Date: December 1988

Section F:

POLICY OBJECTIVE

- Travel costs are the expenses for transportation, lodging, subsistence, and related items incurred by employees who are in travel status on official business of the non-Federal entity. Such costs may be charged on an actual cost basis, on a per diem or mileage basis in lieu of actual costs incurred, or on a combination of the two, provided the method used is applied to an entire trip and not to selected days of the trip, and results in charges consistent with those normally allowed in like circumstances in the non-Federal entity's non-federally-funded activities and in accordance with non-Federal entity's written travel reimbursement policies. Notwithstanding the provisions of § 200.475 General costs of government, travel costs of officials covered by that section are allowable with the prior written approval of the Federal awarding agency or pass-through entity when they are specifically related to the Federal award.
- To control travel expenditures by ensuring that the travel purposes are consistent with program objectives and do not exceed budget.
- To make accounting and reimbursement for travel more efficient for program directors and supervisors who ensure compliance with travel policies.

SPECIFIC POLICY STATEMENTS

1. The Business Office will require the necessary support and documentation for all travel in order to fully comply with federal audit regulations.
2. Reimbursement for a mileage claim for local travel for **official college business** will be submitted for payment on a monthly basis. Mileage should be submitted monthly and not accumulated for several months.
3. A Travel advance authorization for out of area travel must be completed and approved prior to any travel. Documentation such as agenda must be attached.
4. Travel advance amounts for meals, mileage and lodging will follow appropriate GSA rates. Per Diem is only paid for travel that requires an overnight stay.

The regulations are as follows:

Meals and Incidental Expenses (M&IE) Breakdown

The separate amounts for breakfast, lunch and dinner listed in the GSA chart are provided should you need to deduct any of those meals from your trip voucher. For example, if your trip includes meals that are already paid for by the government (such as through a registration fee for a conference), you will need to deduct those meals from your voucher. Refer to [301-11.18 of the Federal Travel Regulation](#) for specific guidance on deducting these amounts from your per diem reimbursement claims for meals furnished to you by the government.

The table lists the six M&IE tiers in the lower 48 continental United States (currently ranging from \$68 to \$92). If you need to deduct a meal amount, first determine the location where you will be working while on official travel. You can look up the location-specific information at www.gsa.gov/perdiem. The M&IE rate for your location will be one of the six tiers listed on this table. Find the corresponding amount on the first line of the table (M&IE Total) and then look below for each specific meal deduction amount.

The table lists examples of the M&IE rate that is provided for incidental expenses (currently \$5 for all tiers).

M&IE total	Breakfast	Lunch	Dinner	Incidental expenses
\$68	\$16	\$19	\$28	\$5
\$74	\$18	\$20	\$31	\$5
\$80	\$20	\$22	\$33	\$5
\$86	\$22	\$23	\$36	\$5
\$92	\$23	\$26	\$38	\$5

This table lists the amount federal employees receive for the first and last calendar day of travel. The first and last calendar day of travel is calculated at 75 percent.

Total	First and Last Day
\$69	\$51.00
\$74	\$55.50
\$80	\$60.00
\$86	\$64.50
\$92	\$69.00

5. Payment requests for registration and lodging must be completed on a check request or prior approval of use of College Credit card(s) with appropriate documentation attached.
6. All airline reservations should have a purchase order or prior approval of use of the College Credit card(s) so that payments may be done on a timely basis. When booking flights only economy class tickets are allowable. In addition, SBC is required by 49 U.S.C. 40118, commonly referred to as the "Fly America Act," to use United States air carrier service for all air travel and cargo transportation services funded by the United States Government. One exception to this requirement is transportation provided under a bilateral or multilateral air transport agreement, to which the United States Government and the government of a foreign country are parties, and which the Department of Transportation has determined meets the requirements of the Fly America Act. This is further defined in criteria 2 of the CFR 200.475.

7. Employees opting to drive for a conference/meeting that requires more than eight hours of driving, will be required to use the lesser of the air fare or mileage for figuring travel costs. Documentation showing the air fare at economy class, must be attached to travel authorization form. Individuals opting to drive will not be paid additional per diem beyond the number of days required if flying. In addition, if the travel occurs during regular work hours the individual will be required to use annual leave for the additional driving days.
8. Employees who opt to extend their stay beyond conference/meeting times, will be required to adequately document the cost of the airfare for returning at required time versus the extended stay. If the airfare costs more for the extended stay the individual will be required to pay the difference. All hotel and other expenses for the extended stay will be paid by the employee.
9. Individuals who use their personal credit cards for car rental, are required to take the additional car rental insurance for their own insurance protection. Car rentals, must have prior approval from the employee's supervisor before payment or reimbursement will be made.
10. If the travel is scheduled to begin on a weekend, round trip mileage is paid from your home. Otherwise for travel beginning on a regular workday, the mileage begins from your workplace. Exception would be if you live in the same location as departure/return.
11. Travel requests should have correct account numbers on form and have a project attached.
12. Within ten working days from return trip, the approved advance authorization travel report must be completed and submitted to their supervisor for approval for any travel expenses incurred to ensure that costs are necessary and allowable. Once approved the supervisor will forward to the business office for processing. Receipts for motel, taxi, airport parking, and luggage fees must be attached to copy of travel authorization. In addition, the employee will be required to complete a summary of their travel and how the travel will assist them in their current positions.
13. Failure to turn in receipts and completing the summary of travel will result in refusal of further travel (and travel advances) or other disciplinary action by the supervisor.
14. Submission of all travel authorizations, payment requests and receipts are the responsibility of the traveler.
15. The College will withhold the full amount of a travel authorization from an employee's payroll check for an employee who receives a travel advance and does not attend the approved travel due to unforeseen circumstances. Employees that received excess travel funds will need to reimburse the college within 10 working days of return from travel. If the employee requests payroll deductions the entire amount owed will be deducted from the first paycheck following their return from travel.
16. All staff and faculty must use a college vehicle when available for local travel within a 100-mile (one way) radius from their work location. No motel fees will be paid for travel within a 100-mile radius unless, approved by administration. In addition, employees who travel under general funds will be required to use a college vehicle for all travel. Exemptions apply to SBC Administration and the Board of Trustees on use of vehicles for local travel.

17. Only employees and students are eligible to ride in all SBC vehicles.

Responsibility:

Vice President of Operations
IT/Finance Director
Accounts Payable Technician
Program Director
Supervisors

Revised: May 2025

POLICY: HUMAN RESOURCES

Date: 2013

Section G:

POLICY OBJECTIVE

- To include all elements necessary to accumulate and maintain personnel information.
- To ensure that all personnel paperwork is submitted in a timely manner.

SPECIFIC POLICY STATEMENTS

1. Human Resources is responsible for all personnel tasks as needed, including advertising of positions, scheduling of interview and all paperwork involved with hiring of an individual as an employee.
2. A request for letter of appointment will be prepared by Human Resources Director and signed by the college President for all-new hires (fulltime or part-time). Request for reassignments of current employees to new positions will be prepared by the Project Director and signed off by the College President.
3. The letter of appointment shall include wage classification data, name of program involved, the account to be charged, the length of employment if temporary.
4. Pre-employment drug testing will be scheduled on Tuesday of every week with the SR Gaming Office. Failure to test, a cancelled test or a positive result of testing will disqualify anyone for employment (Substance Abuse Policy, Chapter VII, Section 17).
5. Background checks will be done through Federal, State, Local and Tribal agencies. Applicants must have a clear driving record to operate college vehicles.
6. Background checks for high risk positions (Day Care and Transit) must not have any charges of assault, child abuse/neglect for the past seven years.
7. Once confirmation is received in the Human Resources Department, the applicant will be informed by letter to start work.
8. The Human Resources Director will maintain all personnel and sensitive files including property title, vehicle title, legal descriptions, and employee benefit information.
9. All new employees must complete appropriate insurance and benefit applications with the Human Resources Director on their first day of employment.
10. If appropriate paperwork or documents are not turned in on a timely manner payroll department has the right to block direct deposit or hold payroll check and employee will have to bring documents in the HR office before check is released.

Responsibility:

Vice President of Operations
Human Resources Manager
Supervisors

Revised: July 2015

POLICY: PAYROLL

Date: December 1988

Section H:

POLICY OBJECTIVES

- Properly control leave payments, accumulate employee hours worked by program or office.
- Calculate pay amounts and withholdings. Accurately prepare and distribute payroll checks and withholding deposits on a timely basis. Prepare reports that are necessary for external and internal reporting purposes.
- To properly distribute payroll expenses to contracts and grants, and to obtain timely reimbursement of all allowable payroll expenditures from the funding agency.

SPECIFIC POLICY STATEMENTS

1. All payroll disbursements will be made by check or direct deposit.
2. Any changes in rate of pay must be documented in a letter signed by the College President. A copy of the letter must be sent to the Human Resources Director so that payroll records can be adjusted to accurately reflect the change.
3. Extra contract checks will be run through payroll for all current employees.
4. A W-4 Form (Employee's withholding allowance certificate must be completed and submitted to the Business Office for the college personnel before the first working day.
5. A Certificate of Employment Eligibility Form (I-9) shall be completed prior to employment with a copy for personnel file. ID forms to be used for I-9 are: US passport, current driver's license, Tribe ID, social security card, original birth certificate.
6. Timesheets for exempt employees (including faculty) will be submitted for record of leave purposes.
7. Timesheets for non-exempt employees will be submitted showing actual hours worked and leave taken.
8. Timesheets must be completed and signed by the individual employee and submitted to the program director or supervisor following the end of each pay period for their signature. Both the employee and the supervisor will be required to date the timesheet.
9. Time & Effort Set-Up Procedures: An employee's time and effort will be documented on an employee's timesheet if paid through several sources. The timesheet indicates the applicable hours and the complete fund number through which the employee is paid. The employee and supervisor must sign and date the timesheet verifying the time and effort for each source of payment for each pay period.

10. Employees that are paid through a sole source on a grant or general fund must sign and date their timesheet along with their supervisor verifying the time and effort of the sole source for each pay period.
11. Any correction made to a timesheet after submission, must be legibly corrected by strike through with the correction beside it and initialed by the employee or the supervisor.
11. The college will have 26 pay periods per year. The pay periods will end on alternating Saturdays.
12. Completed time sheets for all employees and contract payment with memorandum authorizing payment must be approved and signed by program director or supervisor and submitted to the Business Office by 10:00 a.m. on the Monday after the end the pay period or at the date and time specified by the IT/Finance Director.
13. Direct deposit is available to all employees and is encouraged. A copy of a personal check should be submitted along with completion of direct deposit forms. (Do not submit deposit slips)
14. Direct deposits will be available on Wednesday after the end of the pay period. No direct deposit will be issued if a time sheet is NOT turned in or approved on time.
15. Payroll checks will be available on Thursday after the end of pay period. No checks will be issued if a time sheet is NOT turned in or approved.

Responsibility:

Human Resource Manager
IT/Finance Director
Supervisor
College Employees

Revised: July 2023

POLICY: ACCOUNTS RECEIVABLES AND RECEIPTING

Date: December 1988

Section I:

POLICY OBJECTIVES

- To provide for timely and accurate collection and deposit of all funds due to the college. The Vice President of Operations has ultimate responsibility to ensure that all funds due to the college under each contract are received promptly. To use sound cash management practices for the investment of college funds to yield a safe and adequate return.
- To include control elements necessary to properly account for and safeguard the cash of the college.

SPECIFIC POLICY STATEMENTS

1. Computerized receipts will be issued for all payments made to the college. The receipts will be reconciled to the actual deposit made with the bank.
2. All cash received by programs or other departments must be remitted on a daily basis to the college. Account numbers should accompany all cash and checks. Source of funds must be noted on receipts.
3. The Business Office will make weekly deposits for all checks in the bank using eDeposit system. Cash will be deposited as needed.
4. Separate receipt books must be maintained for special accounts.
5. All cash deposits will be reviewed by business office staff to assure accuracy and accountability.
6. The original receipt will be returned to the individual making payments on request.
7. Business Office will accept credit cards (Visa, Master Card, and Discover) for any payments.

Responsibility:

Vice President of Operations
IT/Finance Director
Account Receivable Technician

Revised: July 2023

POLICY: COLLECTION OF STUDENT DEBT

Date: September 2005

Section J:

POLICY OBJECTIVES:

- To ensure fairness to current students who are attempting to pay debt due to tuition, lab fees, books, fees, housing rental fees, travel costs and any other debt owed to Sitting Bull College.
- To ensure effective fiscal management and collection of student debt, as determined by Board of Trustees and to encourage fiscal responsibility by students pursuing a higher education degree at Sitting Bull College.
- It is the policy approved by the Board of Trustees that an official or unofficial transcript or a diploma will not be released until debt is paid in full.

SPECIFIC POLICY STATEMENTS / CONTENT:

1. Every effort will be made by the SBC Business Office to collect any and all debts owed to Sitting Bull College for tuition, books and fees, student housing rentals, travel costs and any other debt owed to Sitting Bull College.
2. At the beginning of each semester, a student who owes Sitting Bull College must enter into a payment agreement with Sitting Bull College
3. Once this form is completed and on file with SBC, the agreement cannot be canceled unless both parties (SBC & Student) agree to cancel the Agreement in writing.
4. A student who is employed shall arrange for a payroll deduction with employer and notify the SBC Business office in writing of the payroll deduction agreement. A student is required to notify SBC if debtor's employment or employer changes, where the debtor will be required to sign a new debt agreement form, including a new payroll deduction agreement.
5. Students who attended prior to fall 2003 and have a debt for tuition, books, and fees to the college this debt has been forgiven as approved by the Board of Trustee as of November 2014.
6. Students who have a recent debt, fall 2003 to current and if a student does not agree with amount owed to SBC, the student may dispute the debt by submitting a letter to the SBC Business Office.
 - a. The SBC Business Office will review debt information with the Financial Aid Director, Registrar and Accounts Receivable Technician to determine if extenuating circumstances exist.
 - b. If extenuating circumstances exist, some of the debt may be written off, except for Bookstore fees.
 - c. If extenuating circumstances DO NOT exist, student will be responsible for entire balance due.

7. Sitting Bull College may collect on student debt beyond two years by one or all of the following methods:
 - a. SBC automatically withhold up to \$200 from excess Title IV financial aid (PELL & SEOG) per academic year, to be used for paying off prior year debt. This withholding will occur during the first semester enrolled during an academic year and will continue to be withheld during the first semester of each academic year enrolled until the debt is paid in full.
 - b. Enter into a payment agreement by completing and signing a Debt Agreement form with the student.

Responsibility:

Accounts Receivable Technician
Financial Aid Director
IT/Finance Director
Vice President of Operations

Revised: July 2023

POLICY: PROPERTY (FIXED ASSETS)

Date: December 1988

Section K:

POLICY OBJECTIVES

- To include all elements necessary to accumulate and maintain property information, control assets by program, and prepare reports that are necessary for external and internal reporting purposes.
- To keep property expenditures within the limitation set by program objectives, budgets, and contract or contract revenues.
- To make the property accounting process more efficient for program directors and supervisors who have the ultimate responsibility to ensure that all property transactions are in compliance with federal, state, local or private contract requirements and college policies.
- To include control elements necessary to properly account for property additions deletions, or transfers and to safeguard college property.

SPECIFIC POLICY STATEMENTS

1. Property purchases in excess of budgeted amounts will not be allowed.
2. Purchases of property must comply with accounts payable and purchasing policies, including regulations for competitive bids.
3. Property acquisitions will be recorded on SBC inventory records (capitalized) of the cost (purchase cost) if each individual item exceeds \$5,000. Property purchases must be provided for in the budget.
4. Property purchase and/or use shall be identified with specific contracts or grants and charged directly to those contracts or grants.
5. All transfers of property between programs and/or locations must be approved by the Vice President of Operations and must comply with grant or contract requirements. Notice of the transfers must be sent to the Vice President of Operations within ten (10) days of the transfer.
6. Disposal of property with initial purchase value of over \$1,000.00 must comply with grant or contract requirements. Notice of the disposal must be sent to the Human Resources Director.
7. All funds received from property disposal will be treated in accordance with grant or contract provisions, where applicable.
8. Leasing of property should be considered as an alternative to purchase. Based on the projected cash flow a decision may be made whether to lease or purchase.
9. Program directors are responsible for all property under their programs.
10. A physical inventory of college property will be taken annually by grant directors and upon the closeout of a grant or contract.

11. Records on all property (including land) owned by the college will be maintained by the Business Office. The property listing for each program will be kept in the program folder.
12. The Business Office will be responsible for calculation of depreciation schedules for indirect cost base.
13. No property may be removed from the premises of SBC, unless for specific use by SBC. Equipment will not be allowed to be rented for any personal use, unless the equipment was purchased with that designation.

Responsibility:

Human Resources Director
IT/Finance Director
Vice President of Operations

Revised: July 2023

POLICY: AUXILIARY BUSINESS POLICIES

Date: July, 2008

Section L:

POLICY OBJECTIVE:

- To provide guidelines for establishment of auxiliary business under Sitting Bull College.
- To assure that the business is viable and able to be self-supporting.
- To enhance the vision and mission of the College.

PROCEDURES:

1. All potential businesses must be approved by administration and the Board of Trustees.
2. Potential businesses should develop a feasibility study to ascertain the whether the business would be successful
3. Potential businesses should develop a business plan along with a marketing plan.
4. Business office will monitor all expenditures of the auxiliary business to assure that business is meeting goals.
5. Business office will develop an incentive policy for each business. Incentive may include 15 percentage of net profits annually, unless otherwise approved by SBC Administration.
6. Business office will be assessing the College’s 20.5% indirect rate through June 30, 2025 for accounting services, after incentive pay is figured.
7. Business managers will report quarterly to Board of Trustees. Report should include a profit and loss statement.

Responsibility:

President
Managers

Revised: July 2023

POLICY: IDENTITY THEFT POLICY

Date: 2012

Section M:

POLICY AND OBJECTIVE:

- To protect employees and students from damages related to the loss or misuse of sensitive information.
- To lower the risk of identity theft and fraud of employees and students and minimize potential damages from such activities.
- To identify what risks may be potentially fraudulent.

SPECIFIC POLICY STATEMENTS:

1. Definitions of sensitive information are as follows:
 - Printed data that may have sensitive information; i.e. any personal information on employee or student.
 - Electronic data storage and distribution with any personal information.
2. Sensitive information can be:
 - Credit card information i.e. number, expiration date, name and address.
 - Tax identification numbers including social security numbers, employer identification numbers and student identification numbers.
 - Paychecks, pay stubs, bank account numbers.
 - Medical information including doctor's name and claims; insurance claims; prescriptions, any personal information
 - Personal information; i.e. date of birth, address, phone numbers, maiden names, and names.
3. In the distribution of hard copy information, all employees will comply with the following:
 - File cabinets, desk drawers, cabinets and any other storage space containing sensitive information will be locked when not in use.
 - Storage rooms containing sensitive information and records will be locked at end of each workday or when unsupervised.
 - Desks, workstations, work areas, printers and fax machines and any common shared work areas will be cleared of all sensitive information when not in use.
 - Discarded documents with sensitive information will be placed within locked shred bin or immediately shredded using appropriate shredding device.
4. Sensitive information regarding any employee or student may not be transmitted via email at any time.
5. Red flags that are potential indicators of fraud are as follows:

- Alerts, notifications or warnings from consumer reporting agency;
- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with employee or student information;
- Identifying information presented that is inconsistent with other information the employee, or student provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a Federal Financial Aid);
- Social security number presented that is the same as one given by another employee or student;
- Notice to Sitting Bull College that an account has unauthorized activity;
- Notice by student to Sitting Bull College of unauthorized access to or use of student account information;
- Notice to Sitting Bull College from an employee or student, identity theft victim, law enforcement or other person that Sitting Bull College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft;
- Student signs a different name on registration forms.

6. Program Administration

A. Oversight

Responsibility for developing, implementing and updating the Program lies with the Governance Committee for Sitting Bull College. The Program Administrator will be the Vice President of Operations who can be reached at (701) 854-8001 and is responsible for ensuring appropriate training of Sitting Bull College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Sitting Bull College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsible steps to be taken when a Red Flag is detected.

C. Program Updates

The Committee will review and update this Program at least annually to reflect changes in risks to employees and students and the soundness of Sitting Bull College from Identity Theft. In doing so, the Committee will consider Sitting Bull College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in Sitting Bull College's business arrangements with other entities.

After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall update the Program.

- D. Oversight of Service Provider Arrangements
Sitting Bull College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedure designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Responsibility:

Human Resources Director
IT/Finance Director
Vice President of Operations

Revised: July 2015

POLICY: GRANT WRITING COMPENSATION

Date:

Section N:

POLICY AND OBJECTIVE:

Faculty and staff should take an active role in identifying potential funding sources for their programs or special projects. A key source is identifying potential grants is the one stop shop created by the federal government: www.grants.gov. Many other sources are available as well and may be obtained through the Vice President of Operations.

As a means of encouraging faculty and staff to assist with seeking funding for their departments the Board of Trustee has approved the following compensation:

Grant Amounts:	Federal Grants payments:	Foundation Grants payments:
\$25,000-100,000	\$2,000	\$1,000
\$101,000-300,000	\$3,000	\$1,500
\$301,000-500,000	\$4,000	\$2,000
\$501,000-700,000	\$5,000	\$2,500
\$701,000-900,000	\$6,000	\$3,000
\$901,000-1,100,000	\$7,000	\$3,500
\$1,101,000-1,300,000	\$8,000	\$4,000
\$1,301,000-1,500,000	\$9,000	\$4,500
\$1,500,000-PLUS	\$10,000	\$5,000

In order to be compensated faculty and staff must work on the grant after regular working hours and must seek approval of the President, have a signed contract in place before submission, and receive approval for submission through the Governance Committee. In addition, payment will not be made for submission for non-competitive grant funding for programs that are allocated specifically for Tribal Colleges. Compensation will be based on 20% at the time of submission and 80% upon notification of award. Continuation award/grants do not qualify for additional compensations. If a faculty and staff are not capable of writing a grant, but feel that the grant will be beneficial to their department, the college will make every effort possible to assist with finding a grant writer and will compensate for writing the grant.

Governance Committee Approval Process:

Faculty and staff must provide the Governance Committee with the following information before a grant is submitted to the funding agency:

- Name of Granting Agency:
- Name of Grant:
- Purpose of Grant:
- Rational of why the grant is needed:

- Goals:
- Strategic Plan Correlation:
- Can get from web site under about us
 - Budget (including match if required and where the match will come from):
- Will you be asking for compensation for writing of grant: ____Yes or ____No
- Do you have approval from your supervisor to write the grant: ____Yes or ____No

The Governance Committee will review the funding opportunity and approve or disapprove the submission. The Vice President will assist with the grant submission and has the authorizing authority for submission of grants for Sitting Bull College. **No proposal can be released for submission without the authorized signature.**

Responsibility:

President

Vice President of Operations

Revised: September 2024

POLICY: GRAMM-LEACH-BLILEY ACT

DATE: February 2021

SECTION O:

SUMMARY:

Sitting Bull College (SBC) is required to maintain a formal information security program in compliance with the Gramm-Leach-Bliley Act (GLBA), which is mandated by the Federal Trade Commission's (FTC) Safeguards Rule. GLBA requires financial institutions to provide security and maintain confidentiality of customer information collected or stored by the institution or their affiliates. Higher education institutions meet the definition of a GLBA financial institution as they may service student loans or offer other financial products or services.

OVERVIEW:

SBC's GLBA Information Security Program is specifically designed to help ensure security and confidentiality of customer financial information as designated by GLBA. Specifically, it is designed to prevent anticipated threats or hazards to the security or integrity of such information, and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

SCOPE:

SBC's GLBA Information Security Program applies to all non-public Personal Identifiable Information (PII) that is part of data, records, documents or other media (including non-electronic media such as paper) about a customer when it also pertains to a financial service or product, when the data or non-electronic media was created and/or is maintained by SBC or on SBC's behalf.

DEFINITIONS:

Covered Data – Data included within the scope of GLBA requirements, both electronic and non-electronic. Examples include customer information related to student accounts, financial aid information, loan data, payroll records, collections, payment plans, etc. when PII (such as SSN, driver's license, date of birth, credit card number) is also included.

Program Officer – The position designated by the SBC Administration with the authority and responsibility of overseeing SBC's GLBA Information Security Program. The Program Officer is authorized to designate other SBC representatives to assume the program's responsibilities.

Data Governance Committee – SBC's governing body (Governance Committee) responsible for the oversight of data, both electronic and non-electronic, created and/or maintained by SBC or on SBC's behalf. The Committee is responsible for administering SBC's Data Classification Policy, which includes Covered Data.

GLBA INFORMATION SECURITY PROGRAM COORDINATION:

The IT/Finance Director is designated as SBC's GLBA Program Officer. All questions concerning SBC's GLBA compliance must be directed to the Program Officer.

The Program Officer is responsible for overseeing and implementing SBC's information security program and enforcing the program in compliance. The Program Officer, in collaboration with SBC Administration and their Data Governance Committee, will determine

the appropriate Information Security Program measures SBC must implement to comply – both directly and indirectly - with GLBA requirements. This includes determining audits, testing, software, services, staffing, training and education, etc.

The Data Governance Committee ensures the SBC’s Data Classification Policy is implemented, which includes access and handling of Covered Data.

GLBA Information Security Program Elements:

Risk Identification and Assessment

The information security program is based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in unauthorized disclosure, misuse, alternation, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

Covered Data risk identification, assessment and inventory of Covered Data is administered by the Data Governance Committee through compliance with the Data Classification Policy. The Policy requires the identification of data elements, including Covered Data. The Policy also requires a review of access controls, preventing unauthorized access, to Covered Data as confidentiality, access and handling constraints are then assigned based on their classifications.

The Program Officer will coordinate the additional GLBA risk identification and assessment activities. Examples of risks needing to be identified and assessed may include Covered Data exposure due to violations of SBC policies, failure to comply with GLBA requirements on devices not managed by the IT department, failure to comply with the SBC’s computing account and password procedures, Covered Data exposures during transmission, business continuity failures (such as natural disasters) and loss of security with non-electronic media (such as unsecured paper documents with Covered Data present).

Information Systems and Safeguards

Physical Security:

Individuals in possession of Covered Data are responsible for the physical security of that data and the media storing that data. An example is the SBC IT department leveraging a secured data center with appropriate environmental controls and secured data backup processes.

Another example is securing offices, desks, and filing cabinets containing Covered Data. The office, department, or individual possessing devices not managed by the SBC IT department used to store Covered Data must document the device type (server, PC, tablet, smart phone, etc.), device identification information and device location, along with what Covered Data is being stored. The device owner must ensure all cybersecurity safeguards are followed as directed by the IT department. An example would be a staff member’s device where a financial aid report that includes Covered Data has been downloaded.

Disposing of Covered Data, such as the shredding of non-electronic media, destruction of electronic storage devices, or erasure of data stored in the cloud by contracted service providers, must comply with the SBC data retention and disposal policies, standards, and procedures.

Information Systems:

A large subset of electronic Covered Data is stored in information systems, including both those developed by SBC and those purchased from service providers. SBC Safeguards for Covered Data are fundamental elements of the risk identification and assessment stated in this document. Covered Data residing in information systems must be a priority for the Data Governance Committee in compliance with the Data Classification Policy, specifically anticipating and evaluating changes to information systems impacting Covered Data.

SBC uses encryption to protect Covered Data both when transmitted over external networks or at rest unless the Program Officer has approved either an exception or alternate protection method. SBC uses or will implement multi-factor authentication for any systems that processes or stored covered data unless the Program Officer has approved either an exception or alternate protection method. Logs will be securely saved and monitored for suspicious activity, wherever feasible, thus ensuring continuous oversight of access to and use of Covered Data in compliance with applicable security standards.

Security and Incident Management

The Program Officer, in collaboration with SBC Administration, the IT department, and the Data Governance Committee, will facilitate the creation and maintenance of the SBC cybersecurity-related policies, procedures, standards, best practices, and guidelines. This oversight extends to the operation of cybersecurity tools (firewalls, anti-virus, advanced email protection, data encryption, MFA, etc.), training and education (both for IT and end users), services, and staffing needed for compliance with all laws and SBC policies.

The Program Officer is also responsible for the SBC incident response plan as required by GLBA, and it is available to previously approved staff upon request.

Employee Management and Training

SBC administers GLBA-related training and education activities with the goal of minimizing risk and maximizing the effectiveness of safeguards for Covered Data. While general SBC cybersecurity training, education, and resources address vital safeguards, users with access to Covered Data require additional GLBA-specific knowledge.

The Program Officer, in collaboration with the Data Governance Committee, data owners and data stewards defined by the SBC Data Classification Policy, ensure users with access to Covered Data, both electronic and non-electronic, are made aware of the importance of GLBA requirements.

These users must be familiar with all laws and SBC policies prior to gaining Covered Data access. These users must be especially acquainted with this document, the list of Covered Data elements for which they have been granted access, and SBC's Data Classification and Acceptable Use Policy.

Oversight of Service Providers and Contracts

External service providers in possession of Covered Data must demonstrate they are taking appropriate actions to safeguard Covered Data as part of the contracting process. Contract language may require service providers to explicitly commit to GLBA compliance.

SBC may also require a service provider to issue results of security audits, proof of certain types of insurance, or other documentation upon request. All service providers will be

obligated to notify SBC when any relevant security incident occurs. Furthermore, service providers must agree that modified GLBA requirements and/or other compliance measures could be required by SBC during any contract renewal.

GLBA INFORMATION SECURITY PROGRAM REVIEW, ADJUSTMENT AND REPORTING:

Program review will be conducted by the Program Officer and the campus Data Governance Committee.

The Data Governance Committee will conduct a semi-annual audit of compliance with the SBC Data Classification Policy as it pertains to Covered Data. The audit will determine if the list of Covered Data elements remains accurate – with a priority being new Covered Data being transmitted to/from external service providers and agencies. The audit will also determine if user access remains accurate. The Committee will direct appropriate adjustments be undertaken, as needed, because of the audit findings.

The Program Officer will conduct an annual review of all other program elements. The Program Officer will inform the review using findings discovered in testing (such as penetration testing), monitoring and audits. The Program Officer will also remain current in GLBA and cybersecurity changes using industry websites, publications, interactions with colleagues, training, conferences, webinars, etc. The Program Officer, in collaboration with SBC Administration, will adjust this document because of the annual review.

The Program Officer and the chair of the Data Governance Committee will report to the SBC Administration annually on the campus compliance level with the GLBA, any changes made in the last year, any steps needed to retain GLBA compliance, and any relevant continuous improvement items for the coming year.

Responsibility:

Vice President
IT/Finance Director

Revised: May 2025

POLICY: DATA CLASSIFICATION POLICY

Date: 2025

Section P:

PURPOSE

The purpose of this policy is to classify Sitting Bull College (SBC) data based on the confidentiality and sensitivity level needed, if any, for various SBC data groups. All members of SBC's community have a responsibility to prevent disclosure of restricted and private SBC data in accordance with this policy.

SCOPE

This policy applies to all SBC data stored in all formats. These include in electronic form (such as any storage device, application, etc.) and in non-digital formats (such as paper). Anyone accessing, storing, providing access, transmitting, adding, modifying and/or deleting SBC data is subject to the policy. This includes, but is not limited to, employees, students, contractors, guests, and others that may interact with SBC data.

POLICY STATEMENT

All SBC data needs to be classified into its appropriate classification category – public, private, or restricted. This policy will provide broad examples of classifications. Individual data owners, in concert with data stewards, will determine and maintain classifications at the data item level as they deem necessary.

However, the classification cannot supersede and must align with governmental privacy regulations – most notably FERPA, HIPAA, GLBA, and PCI. Since governmental data privacy regulations can change frequently and new regulations are sometimes added, this must be a 'living' policy subject to regular review.

ROLES

Data Owners — Individuals with organizational responsibility for SBC unit(s) or department(s) maintained within their area of authority, typically a member of the SBC Administration.

Data Stewards – Individuals who lead and/or direct SBC unit(s) or department(s) and have day-to-day oversight of various numbers of SBC data groups. An example might be a registrar.

Data Custodians – Individuals with maintenance authority (add, modify and/or delete) for various SBC data groups. An example might be a member of the admissions staff. It would also include all users who can add, modify or delete data about themselves (such as a student updating their address online).

Data Users – Individuals with 'read only' authority to various numbers of SBC data groups. Note that an individual can have multiple roles across various data groups. For example, an individual might be a data user of certain data and a data custodian of other data. For example, a worker in financial aid may be a data custodian for financial aid data, a data user for student billing data and have no access to HR data.

DEFINITIONS

Public Data – Any data or information that does not require any protection. Examples include information found on the SBC public website, which presumably include press releases, news items, public directory information, course catalogs, notices about events, admissions

information, athletics, etc.

Private Data – Non-public data that does not rise to the level of control required for restricted data. Although access to private data is limited to a need-to-know basis, exposure of this data would not result in significant violation of a regulation, contract or law resulting in significant harm to SBC or members of the SBC community, in general. Examples include private student academic history or directory data that a student did not consent to being made public, etc.

Restricted Data – Non-public data that requires the strictest protections and safeguards. Restricted data is where exposure could cause significant violation of a regulation, contract or law resulting in significant harm to SBC or members of the SBC community, in general. Examples include Personally Identifiable Information (PII), health-related data (HIPAA), confidential employee information, credit card information (PCI), legal counsel data and interactions unless specifically deemed non-restricted, etc.

Data Groups – Broad categories of datasets by which data owners and data stewards can attach specific data fields, classify those fields, and determine which individuals should have access to those data fields (lists of data custodians and data users). Examples of data groups include:

- Alumni and fundraising
- Facilities
- Fiscal
- Health
- HR
- Legal
- Research/Indigenous Data
- Student (optional sub-divisions for admissions, financial aid, academic history, etc.)

GenAI Tools – Software tools that use generative models leveraging artificial intelligence to generate content. Examples include Microsoft CoPilot, OpenAI, Google Gemini, and Chat GPT.

RESPONSIBILITIES

Data Owners

- Serve as executive sponsor for the data stewards in their area of authority.
- Determine the appropriate classification of data items within their area of authority
- Resolve escalations from Data Stewards or from other Data Owners concerning policy-related decisions related productivity, efficiency, or compliance.

Data Stewards

- Assign appropriate classifications to data items in their assigned data groups, as directed by the data owner.
- Determine list of data custodians and data users for their assigned data groups, along with the level of access.
- Review the classification list for the assigned data groups regularly to ensure new data items are added and classified.
- Regularly audit the user access lists to ensure all needed changes are implemented.
- Create and document standards, procedures and data privacy measures in alignment with this policy and governmental regulations targeted at data custodians and data users.
- Approve access beyond data custodians and data users – such as to third-party entities. An example might be sending private data to a contractor.
- Understand how assigned data groups are impacted by regulations and other SBC policies.

Data Custodians

- Comply with standards, procedures and data privacy measures in alignment with this policy and governmental regulations as determined by data stewards.
- Report violations of this policy and/or governmental regulations to the appropriate data steward.
- Understand how assigned data group datasets are impacted by regulations and other campus policies.

Data Users

- Report violations of this policy and/or governmental regulations to the appropriate data steward.

EXAMPLES OF DATA CLASSIFICATION

Note this is not an exhaustive list. Data stewards should maintain complete lists for data groups of which have day-to-day oversight.

Public Data Examples

- Public information found on the SBC public website
- Press releases/news items
- Public directory information
- Course catalogs and schedule of classes
- Notices about events
- Admissions information
- Athletics website
- List of employment opportunities
- Public financial data

Private Data Examples

- Private research data
- Library circulation records
- Non-public policies, procedures, guidelines and best practices
- Internal communications
- Internal reports
- Admissions applicant records
- Family Educational Rights and Privacy Act (FERPA)-protected data
- Certain HR-related data, such as employment applications, benefits information, personal contact information
- Non-public donor information
- Non-public facilities information
- ID numbers assigned to SBC campus members

Restricted Data Examples

- Computing account passwords and encryption keys
- Access codes, biometric data
- Export controlled data
- Privileged attorney-client communications
- Personally Identifiable Information (PII) (social security numbers, driver's license numbers, banking account numbers, passport and international student-related numbers)
- Health-related data
- Confidential employee information
- Credit card information (PCI)
- Non-public law enforcement-related data

REGULATIONS ON THE USE OF RESTRICTED AND PRIVATE DATA

- Follow all applicable regulations (FERPA, HIPPA, GLBA, PCI, etc.).
- Do not enter any restricted or private data into GenAI tools unless full compliance with all regulations is confirmed.
- Protect private and restricted data with strong passwords, multi-factor authentication and encryption (both at rest and in transit) when possible.
- Proactively audit user access to ensure no unauthorized users have access.
- Avoid disclosing data unless required by an authorized individual or on a strict need-to-know basis for legitimate business operations.
- Non-electronic data in a location with controlled access such that only authorized parties can obtain access.
- Should be properly destroyed when no longer needed or required.
- Avoid storage of data on any personally owned device or on cloud storage not managed by SBC.
- Avoid storing on mobile storage devices.

COMPLIANCE (“WHAT HAPPENS WHEN SOMEONE VIOLATES THIS POLICY?”)

Users who violate this policy may be denied access to institution computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the institution disciplinary procedures applicable to the user. The institution may suspend, block, or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so as to protect the integrity, security, or functionality of institution or other computing resources or to protect the institution from liability. The institution may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Responsibility:

IT/Finance Director
Vice President of Operations

Revised:

POLICY: INCIDENT RESPONSE PLAN

Date: May 2025

Section Q:

Purpose

This plan is intended to comply with the Gramm-Leach-Bliley (GLBA) Information Security Program requirement that Sitting Bull College (SBC) possess an Incident Response Plan.

Scope

This plan applies to all incidents impacting the SBC IT environment.

Definitions

The SBC Incident Response Team ('The Team') – The SBC Incident Response Team governs, maintains, implements, and activates this plan. Team membership is determined by the SBC Administration. The SBC Incident Response Coordinator serves as the Team Lead.

The SBC Incident Response Coordinator – The SBC's Incident Response Coordinator serves as the Team's lead and is designated by the SBC Administration. The Coordinator ensures the Team performs its duties in a timely and comprehensive manner, as well as other leadership activities.

The SBC IT Environment – The IT environment consists of all SBC-owned and/or operated IT-related equipment, devices, network, servers, storage, IT facilities, software, and services. Examples include, but are not limited to, all components of the SBC computing network, email accounts, cloud-based applications or storage, learning management systems, ERP/student information systems, ancillary applications, and SBC-issued PCs, laptops, servers, phones, tablets, etc.

Data Governance Committee – SBC's governing body responsible for the oversight of data, both electronic and non-electronic, created and/or maintained by SBC or on behalf of SBC. The Committee is responsible for administering the SBC Data Classification Policy.

Users – Individuals currently assigned a SBC computing account or others provided access approved by the SBC IT Department.

Preparation

The Team governs, maintains, implements, and activates this plan. Some examples of activities the Team may perform to comply with this responsibility are:

- Refining Team membership, roles, responsibilities and authority on a regular basis to ensure membership remains accurate and that membership changes are formally communicated to relevant stakeholders.
- Determining, in collaboration with the SBC IT Department, the minimum potential severity level of an incident that would require this plan to be activated.
- Determining, in collaboration with the IT Department, incident triage steps and incident classifications. The classifications should be primarily based on the potential for large-scale sensitive or confidential data exposure as defined by the SBC Data Classification Policy. A secondary categorization should be established based upon the impact of the IT environment's performance and integrity – such as access to key applications by many users.
- Creating a communications plan for incidents based on incident categorization. Communications include any confidential, sensitive and public-facing messaging to both internal and external stakeholders.
- Establishing the incident tracking tool so all individuals responding to an incident can document their findings and activities both for just-in-time and long-term purposes.
- Conducting regular testing of this plan, such as via tabletop exercises. Testing should include testing of the communications plan and the incident tracking tool.

- Becoming acquainted with Special Publication 800-61, Revision 2 as published by the National Institute of Standards and Technology (NIST).
- Becoming acquainted with any compliance requirements in reporting certain incidents to the authorities – both internal and external parties.
- Establishing a predetermined campus location and ensuring it is properly equipped for Team members and others to gather, as appropriate, for incident response activities.
- Creating and maintaining accurate procedures tested as part of tabletop exercises.
- Maintaining contact information (preferred and alternate methods of contacting, if possible) for incident response contributors, including on-call responsibilities during off hours:
 - IT Department
 - The Team
 - Miscellaneous (contact dependent on specific incident classification)
 - The SBC Administration
 - Data Governance Team members
 - Data Owners and Data Stewards
 - SBC police/external law enforcement and legal resources
 - Public Relations
 - External Resources – such as service providers to support the IT Department

A primary goal of incident response is to reduce the number of incidents. The following are examples of action steps the Team may facilitate to assist in meeting this goal:

- Ensuring all users of the SBC IT Environment have available resources to become familiar with SBC policies, procedures, standards, guidelines, and best practices, especially as it pertains to the Appropriate Use and Data Classification Policies.
- Ensuring all users of the SBC IT Environment have access to adequate and timely cybersecurity awareness education materials based on their access to SBC Information Technology Resources and sensitive/confidential data as defined by the SBC Data Classification Policy.
- Supporting the IT Department in meeting its obligations in executing this plan.

While the IT Department has primary responsibility for the detection, analysis, containment, eradication, and recovery from incidents, there is substantial IT preparation needed for the IT Department to be successful in those activities.

The IT Department must procure various tools, receive adequate training, and dedicate staffing possessing specialized skill sets. Examples of tools may include, but are not limited to, firewalls, forensics, advanced email protection, identity and access management, anti-malware, multi-factor authentication, endpoint device management, disaster recovery/business continuity, data encryption, and network monitoring tools.

Additionally, the IT Department must prepare by ensuring that the service providers that assist in incident response activities are qualified and are available in a timely manner, as needed. This includes identifying providers and ensuring contractual procedures are in place.

Detection and Analysis

The IT Department has primary responsibility for detecting and analyzing incidents. Some examples of IT Department compliance activities are:

- Informing the Team when an incident requiring this plan to be activated has occurred.
- Documenting findings and activities in the incident response tracking tool as the means of keeping the Team informed of incident status, as well as for long-term purposes.
- Monitoring the SBC IT environment, both by monitoring tools and from communications received by user(s) reporting system degradation, loss of service, suspected data exposure or breach,

concerns about actions either they or another user may have taken (such as responding to a suspected phishing scheme).

- Conducting incident triage and classification using standards established in collaboration with the Team.
- Collecting evidence of the incident for analysis both during and in review of the incident.
- Involving external service providers, as needed.

Containment, Eradication, and Recovery

The IT Department has primary responsibility for containment, eradication and recovery from incidents. Some examples of IT Department compliance activities are:

- Documenting findings and activities in the incident response tracking tool as the means of keeping The Team informed of incident status, as well as for long-term purposes.
- Executing its role in the implementation of this plan, especially in providing subject matter expertise to the Team and other stakeholders.
- Involving external service providers, as needed.
- Isolating or shutting down of impacted or potentially impacted portions of the SBC IT environment, including all portions, if warranted. This may include disabling, or ‘wiping’ devices assigned to individuals (PCs, tablets, laptops, smartphones, etc.).
- Disabling computing accounts or restricting access, as appropriate.
- Determining recovery steps – such as applying patches, performing upgrades, restoring data, invoking business continuity measures, etc. – if warranted.
- Determining when to return the IT environment and user access to normal operations.

Post-Incident Activity

The Team will:

- Retain all relevant evidence (hardware, software, logs, forensic material, messages, etc.) with specific focus on that which may be of value for any legal-, compliance-, contractual, - and/or other investigatory-related action steps.
- Create a formal Incident Report to be made available on a strict need-to-know basis. This report must include relevant incident details and timelines. It must also include details concerning the Team’s incident response activities and “lessons learned” from the response so the Team can refine its processes, if needed.
- Create a Recommended Continuous Improvement List of additional steps to reduce the risk of future incidents. Document cases where the Team was unable to reach consensus. This list must include all recommended investments in tools, training, services, etc. as well as additions or modifications to policies, procedures, standards, guidelines, and/or best practices. Document cases where the Team was unable to reach consensus.
- These recommended steps may include, but are not limited to, changes to the following:
 - User Training
 - IT staff professional development
 - Added priority for incident prevention
 - Software tools
 - Third-party services
 - Organizational structure changes
 - Personnel-related items (job descriptions, professional development, staffing, etc.)
 - Team governance (membership, structure, roles, responsibilities, scope, etc.)
 - Testing of this plan (timing, scope, scale, external resources needed, etc.)
- Conduct a formal Incident Report and Recommended Continuous Improvement List meeting with the SBC Administration. The meeting should take place after Administrators have had adequate time to review the report and list.
 - Item 1: The Team will present, discuss and respond to questions about the Incident Report. The primary goal is for the SBC Administration to enhance its understanding of

the incident as well as SBC's preparation, detection, and response, and how the Team plans to refine its processes, if needed.

- Item 2: The Team will present, discuss and respond to questions concerning the Recommended Continuous Improvement List. The goal is for the SBC Administration to accept, reject, or modify the recommendations as well as determining actions, if any, for items where the Team could not reach consensus.

Responsibility:

Administration

Revised:

POLICY: RECORDS MANAGEMENT/RETENION/BUSINESS OFFICE

Date: 2013

Section R:

- To provide procedures for retaining and destroying of all financial records of the College
- To insure the confidentiality of records kept on file and records that are destroyed.

SPECIFIC POLICY STATEMENTS

1. The Business Office is responsible for all financial records of the college including accounts payable, accounts receivables, general ledgers, payroll and personnel files, and all health and benefit files.
2. The Business Office will keep a list of all records being kept and stored and those records that will be destroyed on an annual basis.
3. Following is the list of records and years to be retained or destroyed:

Accounts payable ledgers	7 years
Accounts receivable ledgers	7 years
Audit reports, financial statements	Permanent
Bank reconciliations	3 years
Bank statements	3 years
Checks	7 years
Contracts and leases	7 years
Duplicate deposit slips	1-year
Employee Personnel records	
(from date of termination/resignation)	3 years
*Grant files	
(from submission of final grant report)	3 years
*Unless otherwise indicated by granting agency	
Insurance policies	3 years
Inventories/depreciation schedules	7 years
Internal audit materials	3 years
Invoices/checks for vendors	7 years
Payroll records	7 years
Property appraisals	Permanent
Property records	Permanent
Purchase orders	7 years
Student receivable records	Permanent
Tax returns	Permanent

4. The Business Office will plan for destruction of records on a annual basis.

Responsibility:

- Human Resources Director
- IT/Finance Director
- Vice President of Operations
- Grant Directors

Revised: September 2024

POLICY: OUTSTANDING CHECKS POLICY

Date: April 2, 2015

Section S:

POLICY OBJECTIVES

- To assure the proper handling of checks which have been written but have not cleared the bank in a timely manner.
- To assure that all checks written have the notation printed on the face that it is void after six months.

SPECIFIC POLICY STATEMENTS

1. When a check becomes stale dated the payment requestor will be contacted to determine if the check should be voided or reissued.
2. If a check has been reported lost or destroyed the check will be voided and deleted from the Positive Pay system and a replacement check will be re-issued.
3. Voided checks will be credited to the appropriate accounts. If the voided check is from a grant that has been closed out, the money will be reallocated to use for the same purpose as the grant requirement, unless the check is for \$700 or more. If the voided check is over \$700, the granting agency will be contacted on the process to either refund the agency or on how to reuse the funds.

Responsibility:

Administration
IT/Finance Director
Accounts Payable Technician

Revised: July 2023

POLICY: INVESTMENTS

Date: February 1, 2018

Section T:

PURPOSE

The purpose of this investment policy is to assist the Board of Trustees to effectively monitor and evaluate its investment portfolio. The policy will also provide direction and guidance to College administration and the investment advisor.

GENERAL POLICY STATEMENT

Sitting Bull College manages a diversity of investment funds. Each fund is unique and has specific constraints it must operate within. These constraints determine the types of investments allowable and the use of the funds. The intent of these policies is to ensure the investment of these funds meets all established Federal Guidelines and the amount of return on investment is maximized within the constraints of the guidelines established for each fund.

The Board of Trustees has the responsibility for policy development and review. They are primarily responsible for the funds and its objectives. Administration has the responsibility to operate within the constraints established by the Board of Trustees, in relation to day-to-day activities within the investment funds.

Any investment advisor must be a registered investment representative, an insurance company or a bank representative. Any investment advisor must be approved by the Board of Trustees.

BACKGROUND

The College presently has six (6) designated and segregated funds:

- Endowment Fund (Federal)
- Interest Account (Non-Federal)
- Scholarship Fund (Non-Federal)
- Title III Endowment (Federal)
- Maintenance and Operation Endowment (Non-Federal)

Additional designated fund will be established as needed.

GENERAL OBJECTIVE OF EACH FUND

The College seeks three primary objects for its portfolio.

- Maintain sufficient liquidity to meet financial obligations
- Earn a market rate of return (subject to investment constraints)

- Diversify investments among asset classes to ensure safety of principal detailed guidelines for each fund will be attached as part of this policy. The establishment of any new investment fund will be approved by Board of Trustees.

PERMITTED INVESTMENTS

Federal Funds

- In obligations of the United States, or in obligations or securities that are guaranteed or insured by the United States, or mutual (or other) funds registered with the Securities and Exchange Commission and which only invest in obligations of the United States, or securities that are guaranteed or insured by the United States; or
- Deposited only into accounts that are insure by and agency or instrumentality of the United States, or are fully collateralized to ensure protection of the funds, even in the event of a bank failure; or
- Direct obligations of, or obligations the principal of and interest on which are unconditionally guaranteed by, the United States of America or Certificates or receipts established by the United States government or its agents; or
- Instrumentalities representing direct ownership of future interest or principal payments of direct obligations of, or obligations fully guaranteed by, the United States of America or any of its agencies instrumentalities, the obligations of which are backed by the full faith and credit of the United States.

Non-Federal Funds

- Non-federal funds will be invested as follows: **60% stock/40% bond.**

PROHIBITED INVESTMENTS FOR FEDERAL FUNDS

- The portfolio may not deal in the options, short sales, commodities or margin transactions.
- No private placements shall be held in the portfolio.
- No equity holding in the portfolio may exceed 5% of the outstanding voting shares of the issuing corporation without the approval of the Board of Trustees.

CONFLICT OF INTEREST

Officers and employees involved in the investment process will refrain from personal business activity that could conflict with proper executive of the investment program or which can impair their ability to make impartial investment decisions. Officers and employees involved in investing College funds shall disclose to the Board any financial interest in the investment company or in any entities in which investment are being made.

REVIEW AND REVISION OF POLICIES

A report on the investments performance for all funds will be made annually to the Board of Trustees on a fiscal year basis.

Responsibility:

Vice President of Operations

Revised:

INTRODUCTION FUNDRAISING POLICIES & PROCEDURES

The Sitting Bull College Fundraising Policies and Procedures were first formalized in draft on March 18, 2016 by the College's Business & Fundraising Committee. In recognizing the need for enhanced efforts towards self-sufficiency and collaborative standards, the Committee's Strategic Plan was designed to start from the basics of instituting a formalized way of operating in this arena. These Policies & Procedures are meant to serve as the general operating standards for fundraising and related efforts at the College. As with all Policies & Procedures, these are mutually inclusive.

REGULATORY INFORMATION & LANGUAGE

Sitting Bull College, hereafter referred to in Policies & Procedures as the "College", is committed to acting with acceptable Federal, State, and Tribal standards. In these Policies & Procedures the words "donation" and "donor" are used. This is because the College is a qualified charitable organization under the Internal Revenue Service, thus when cash or property is transferred to the College it can be considered as a donation. Donations can usually be deducted from taxable income and the College as part of these Policies & Procedures does include in the Acknowledging Donations Policy a letter to be mailed out to donors specifically stating the amount of the donation or describing donation as well as the College's taxpayer identification number, however the College will not under any case take any responsibility for financial advising of donors; donors should confer with their accountants to do what is right for them.

There may be entities that are not qualified charitable organizations affiliated with the College in whatever regard that use this manual as a basis and those entities should substitute herein the word "donation" for the word "gift" wherever it is used, and "donor" for "giver [of gift]" wherever it is used. Tax rules on gifts are different from donations; givers of gifts should refer to their accountants for information regarding related tax policy.

The fundraising efforts included herein are distinguished as efforts in which Sitting Bull College is the intended beneficiary. Other events in which College employees may partake or are held on Sitting Bull College property should not be construed as College events nor may the College's IRS status be used for any such activity.

POLICY: INITIATING FUNDRAISING EFFORTS/SOLICITATION

Date:

Section U:

POLICY OBJECTIVES

- To streamline ability of College employees or contractors to handle fundraising efforts
- To ensure efforts in accordance with the College's Mission and Vision and other existing policies, as well as enhancing of visibility and image of the College

SPECIFIC POLICY STATEMENTS

1. Sitting Bull College considers fundraising efforts to be any organized activity or solicitation of donations, donations including but not limited to equipment, materials, supplies, services, credit card/cash payments, or pledges, given freely and without expectation of any kind of return or remuneration.
2. Donors are encouraged to support areas reflecting their interests. The College's priorities include donations for unrestricted (General Fund) firstly, followed by restricted and endowment purposes, prior to the acceptance of donation(s) donor may specify desired use and the College will act within ability to designate funds accordingly. Due to the potential for changes within the College due to any number of factors, for example the ending of a program or the necessity to change building plans, changes may be made to where donations are applied. In such cases the College will be as forthright as possible but cannot guarantee that donors will be informed nor agree with changes in which case the College will do what is best for the institution and not the donor.
3. Donors wishing to endow a scholarship will need to contact the financial aid office to start the process. Currently, scholarship endowment(s) have a two (2%) percent administration charge, scholarship funds do not have an administrative charge. Scholarship endowment(s) have a minimum of twenty-five thousand (\$25,000.00) dollars donation requirement, scholarship funds do not have a minimum requirement. Scholarship Endowments must be in full amount with 3-5% allocation based on earnings the prior year for use in the following fall semester. Scholarship endowments and funds both require written agreements.
4. Before pursuing formal discussions with any potential donor for the cash support or for major in-kind (non-cash) gifts for any program/project, there should be conversations with the appropriate department, if applicable, where the donation is going, the Resource Development Office to start the Acknowledging Process, and the Finance Director to determine appropriate handling.

Responsibility:

Administration

Governance Committee

Revised: May 2025

POLICY: DONATION ACCEPTANCE POLICY

Date:

Section V:

POLICY OBJECTIVES

- To provide comprehensive overview of policies relating to acceptance of donations including but not limited to: securities, personal property, real estate, intellectual property, restricted gifts, planned/deferred gifts, in-kind gifts
- To ensure donations fit the organization’s mission and do not have undue costs associated, and to ensure those donations which are not a good fit for the College are handled in a way that maintains a positive relationship with major donors and helps them to understand that some restrictions on gifts may actually render them less useful to College

SPECIFIC POLICY STATEMENTS

1. If the maintenance costs outweigh its value or the gift has too many strings attached the decision can be made to reject the donation. This can be true of gifts of real estate and tangible property, such as boats or stamp collections, and gifts of unusual or unpalatable restrictions.
2. Donations must be approved for acceptance in accordance with the following based on the total amount or annual amount, whichever is more:

Donation amount/value:	College bodies that must agree to acceptance of donation:
\$1,000 and below	Finance Office Administration
\$1,000 - \$4,999	Finance Office/Administration
\$5,000 - \$9,999	Finance Office Administration
\$100,000 and above	Finance Office Administration Board of Trustees

3. Donors can request and be provided with an electronic .PDF copy of the most up-to-date Policies & Procedures. All donations above \$100,000 should include documentation that the donor has received a copy and agrees with the Policies & Procedures.
4. When gifts with restrictions are accepted, restrictions will be prioritized but not guaranteed. These restrictions should be detailed in the donor’s gift or pledge

commitment letter along with donation. Restrictions after initial donation made are subject to approval of Administration.

5. The College will only accept nonpublic traded securities after consultation with auditor and/or legal. A qualified appraiser must determine the fair market value of the securities. The College should explore methods of immediate liquidation of the securities through redemption or sale before accepting the donation. The College should not commit to repurchase or sell closely held securities until the gift of the securities is complete, as the transaction might be viewed by the IRS/CRA as a sale rather than a gift, with adverse tax consequences for the donor.
6. Multiyear pledges are encouraged but reasonable time periods should be considered. Pledge commitment forms must be completed for multiyear pledges.
7. Donations of tangible property should have a use related to the College's tax-exempt purposes. Donations of jewelry, artwork, collections, equipment and software should be approved if possible only after consultation of any College employees with direct or departmental knowledge of subject (for example, librarian should be consulted on rare books donations, vehicle donations should be inspected prior to acceptance by Service Center. Such donations must be used by or sold for the benefit of the College. If donations are sold, the organization must follow all IRS/CRA requirements for disposing of gifts of tangible personal property and filing the appropriate tax reporting forms.
8. Any donation of property worth more than \$5,000 in the United States requires an appropriate appraisal, which will be paid for by the donor.
9. In-kind donations that are used as grants match should firstly follow Grants Policies & Procedures. The College accepts donations in-kind that support its mission, are consistent with its policies and are properly accounted for and acknowledged. An in-kind donation is a service to the College without charge or consideration. Donors must complete an in-kind form that includes the name of the donor, a description of the service(s), the retail value of the service(s) and permission to publicly recognize the donation.
10. The College reserves the right to dispose of or discontinue acceptance of any donation(s) without notification to donor(s).
11. It is the responsibility of donors that all stipulations and requests should be worked out prior to the College's acceptance of the donation(s).

PROCEDURE

1. Send all donations to Finance/Resource Development for recording,
 - a. Update donor information in the database if the information on the check and/or response form is different.
 - b. Record gifts according to the donor's intended use, i.e. unrestricted, restricted (specific program or project), endowment, etc.

- c. Record in the system the source of the gift, i.e. direct-mail appeal, special event, personal solicitation, etc.
2. Forward on to appropriate party:
 - a. If monetary, forward to Finance Office for accounting and depositing.
 - b. If an object, forward to appropriate department (ie Library or Visitor Center)
3. Prepare biannual report of gifts to be circulated to Governance Committee, Administration and Board of Trustees
4. Acknowledge all gifts in accordance with Acknowledging Donations policy.

Responsibility:

Administration
Governance Committee

Revised: May 2025

POLICY: DONOR PRIVACY

Date:

Section X:

POLICY OBJECTIVES

- To ensure donor requests for privacy measures are handled professionally and confidentially.
- To offer security to donors when providing personal information that their information will be protected at the level they request.

SPECIFIC POLICY STATEMENTS

1. The personal information of all donors, including addresses etc., whether or not donor has requested privacy, must never be sold.
2. In the event donors choose for their names or donations to remain anonymous, requests must be submitted in writing prior to the College accepting the donation. Requests submitted afterward will be considered.
3. If a donor has chosen to remain partially or wholly anonymous their information may still be available to the following persons to ensure their request is handled: Resource Development Officer, Administration, Finance Director. The College may act against any of these specified individuals if disclosure after a written request for anonymity takes place.

Responsibility:

Resource Development Officer
Administration
Finance Director

Revised: May 2025

POLICY: DONOR RECOGNITION

Date:

Section Y:

POLICY OBJECTIVES

- To show gratitude on behalf of the College for donations by providing appropriate level of recognition to donors

SPECIFIC POLICY STATEMENTS

1. Donor Recognition only applicable in accordance with Donor Privacy policy. The College reserves the right to express gratitude to donors and/or for donations unless a request for anonymity/privacy has been submitted prior to acceptance of donation.
2. A selection of named or commemorative gift opportunities may be made available to each donor. Such opportunities represent a tangible means of demonstrating an individual donor’s investment in the College.
3. Donors may request additional recognition and the College will attempt, though not guarantee, to accommodate such requests.
4. All donor recognition must be factually accurate and only based on accepted donations.
Future/promised donations, though appreciated, will not constitute grounds for recognition in any case.
5. Future/promised donations, though appreciated, will not constitute grounds for recognition in any case.

Responsibility:

Resource Development Officer
Administration

Revised: May 2025

POLICY: ENTERING/RECORDING DONATIONS

Date:

Section Z:

POLICY OBJECTIVES

- To streamline ability of College employees or contractors to handle entering and recording donations through software program.

SPECIFIC POLICY STATEMENTS

1. Donations and contributions are monetary contributions made to the College, often from individuals.
2. Grants and Scholarships are typically monetary donations that come from other organizations and often have restrictions on their use, such as a government grant. Sponsorships are donations from an organization or business in exchange for promotion, such as displaying a banner at a fundraising event.
3. Program service fees are fees charged for the services they provide.
4. In-kind contributions are non-monetary donations to the College and might include food donations to the College's food pantry.
5. Donations and contributions will be entered into the College's Jenzabar system for recording purposes by the finance office.
6. Finance office will forward a copy of check, money order, PayPal and or any other electronic means currently being utilized by the College to the Resource Development Office for acknowledgement.
7. Reports of the account(s) must be made available to the college administration upon written request.

Responsibility:

Resource Development Officer
Finance Office

Revised: May 2025

POLICY: ACKNOWLEDGING DONATIONS

Date:

Section AA:

POLICY OBJECTIVES

- To efficiently and effectively provide acknowledgement to donor of College acceptance of gift and expression of gratitude
- To provide donor with statement (legal acknowledgement) for donor's tax purposes for any accepted donations

SPECIFIC POLICY STATEMENTS

1. Donations must be formally accepted to be acknowledged. The College has no obligation to accept a donation.
2. The College should immediately create an Acknowledgement letter upon acceptance of donation.
3. Only a description of any property donated will be provided by the College, unless there is written justification provided for establishing value. Written justifications must be kept by the College for 5 years after date of donation acceptance.
4. Value must not equal or exceed donor benefit (for example: if the donor pays \$40 to eat at a College fundraising event. Printed on the ticket is "Contribution-\$40." If the regular price for the dinner is \$10, the College must disclose the contribution is \$30 (\$40 payment – \$10 regular price. Similarly, if a person pays an amount to participate in an event that is equal to the fair market value cost of the event the payment is not deductible and should not be accepted).
5. The College cannot provide any goods or services to the donor in exchange for all or part of the cash or property contributed for it to be a donation. Acknowledgement letter should contain this information.
6. Donors have a right to request a copy of their acknowledgement letter.
7. Corporate recognition to be negotiated. Private donors will be recognized at Recognition levels below if they so desire. Donors at any level are welcome for a complementary tour of the College campus subject to Administrative approval and availability of tour guide.

Recognition levels:

- a. Cannupa Yuha (pipe carrier) (\$1 million plus) Recognition ceremony at Graduation, reception with College Administration and Board of Trustees, profile in annual report and campaign publications, naming opportunity to be selected, select College merchandise, website recognition, personal letter from President.

- b. Itancan (leader/chief) (\$100,000 – \$999,999) Recognition ceremony at Graduation, reception with College Administration and Board of Trustees and profile in annual report and campaign publications, select College merchandise, naming opportunity to be selected, website recognition, personal letter from President.
- c. Čhante Ohetika (brave heart) (\$25,000 – \$99,999) Recognition ceremony at Student Summit, reception with College Administration and Board of Trustees, profile in annual report and campaign publications, select College merchandise, naming opportunity to be selected, website recognition, personal letter from President.
- d. Oitančan Owečinha (continued leadership) (\$10,000 – \$24,999) Recognition ceremony at Student Summit, profile in annual report and campaign publications, select College merchandise, naming opportunity to be selected, website recognition, personal letter from President.
- e. Otakuye Waste (good relative) (\$5,000 – \$9,999) Listing in annual report and campaign publications select College merchandise, naming opportunity to be selected and website recognition personal letter from President.
- f. Akičita(\$1,000 – \$9,999) Listing in annual report and campaign publications and recognition on website, select College merchandise, personal letter from President.
- g. Tatanka (\$500 – \$999) Listing in annual report and campaign publications, select College merchandise, and recognition on website. Letter from President.
- h. Tiospaye (\$1– \$499) Select College merchandise upon request. (Letter from President)

Responsibility:

Resource Development Officer
Administration

Revised: May 2025

POLICY: USE OF SITTING BULL COLLEGE NAME, LOGOS, IMAGRY, OR OTHER IDENTIFYING INFORMATION

Date;

Section AB:

POLICY OBJECTIVES

- To ensure reputation of the College is protected by responsible use of College information for any effort in which the College engages that could obtain or jeopardize future obtainment of donations.

SPECIFIC POLICY STATEMENTS

1. As Sitting Bull College name and logo is representative in certain aspects of not only the College, but can be construed as representative of the Standing Rock Sioux Tribe under which the College is chartered and the broader Tribal College Movement to which the College belongs as well as its partners and others, it is therefore important that any representation of the College to enhance its image in a way consistent with the Vision and Mission and existing Policies & Procedures and if possible to the benefit of related parties.
2. The Federal Education Rights and Privacy Act (FERPA) must be looked to as the required standard by which to govern the release any student images or information.
3. The College logo(s) and related information are available for use by general College employees and the employees who use these are therefore responsible for their use and required to, excluding Administration, request permission for large scale efforts from their supervisors and bring forward any questions on usage immediately.
4. Branding standards for approved usage must be followed.

Responsibility:

Administration

Board of Trustees

Revised: May 2025

POLICY: PROHIBITED ACTIVITIES

Date:

Section AC:

POLICY OBJECTIVES

- To provide information in addition, and not to be considered complete, to what is written in other Policies specifically related to prohibited fundraising activities.

SPECIFIC POLICY STATEMENTS

1. Even when a fundraising activity is not one that benefits the College directly or is sanctioned by the College, without specific Administrative approval, members of the College community are prohibited from engaging in the following tactics and activities:
2. Using information from the College telephone, email, or any other directory to compile calling or mailing lists for non-College related purposes.
3. Using one’s status as a College employee or student to secure a donation commitment outside of sanctioned activity and/or for any purpose in which the College is not the beneficiary.
4. Conducting gambling as means by which to raise donations without approval of Tribal Gaming Office.

Responsibility:

Administration

Revised: May 2025