

CAU Project Charter Document

Project Name: Data Stewardship (Data Standards and Information Security Systems Advisory Committee)

Project Manager: Tarji Kinsey, Sr. Data Specialist/Key Performance Indicator (KPI) Manager (Office of Institutional Research)

Project Sponsor: Dr. Narendra Patel, Office of Planning, Assessment, and Institutional Research (OPAR)/ Dr. Peter Nwosu, Academic Affairs

Primary Customer: Clark Atlanta University - Information Technology Executive Council (ITEC) Advisory committees

CAU Charter Ref # _____ From **Executive Committee Approved Projects Log**

Description of Project Manager and Responsibilities: The primary role of the Project Manager will be to serve as a liaison between the Data Standards and Information Security Advisory Committee ("The Committee"), the ITEC, other Advisory Committees, and the OITC.

The responsibilities of the Project Manager will include, but are not limited to:

- serve as co-chair of the Committee; provide leadership and accountability for accomplishing the project task assigned to the Committee
 - serve as a non-voting member of the ITEC
 - collaborate with the chairs of the other Advisory Committees to actively communicate and provide data support feedback
 - submit all necessary project related reports to ITEC
 - deliver the Data Standards committees' charge and expectations to each of its' ad hoc committees
-

Prepared By

Document Owner(s)	Project/Organization Role
Tarji Kinsey	Project Manager/Co-Chair of Data Standards Committee/OPAR Representative
Dr. Narendra Patel	Assistant Vice President for Planning, Assessment and Institutional Research/ SACSCOC Accreditation Liaison
Dr. Lauren Lopez	Executive Director of Institutional Assessment & Effectiveness

Project Charter Version Control

Version	Date	Author	Change Description
.5	12/18/2017	Tarji Kinsey	Pre-Submission – This is the initial submission of the project charter

1 SCOPE: PROJECT PURPOSE & JUSTIFICATION

The purpose of the Data Stewardship project will be to provide centralized support for audit, compliance, and internal/external reporting needs to the other CAU Advisory Committee projects. Additionally, this project will further promote the mission of the Data Standards and Information Security Advisory Committee ("The Committee"), which is to evaluate, interpret, and make recommendations regarding the University's data standards and controls.

Clark Atlanta University currently uses the Banner Enterprise Resource Planning (ERP) system along with a host of integrated/non-integrated applications to record and maintain data for their students, institutional and non-institutional employees, and financials. Banner has functionality for five modules. However, CAU utilizes four of the available five modules: Banner Student, Banner Finance, Banner Human Resources, Banner Financial Aid (*partially used*), and Banner Advancement (*not used*).

It is also common to use outside [of Banner] applications and "shadow" systems that users record and maintain data for students, employees, alumni/donor, faculty qualifications and credentialing, etc. Some of the applications/systems that are not integrated with Banner and are merely resident within a department or possibly, resident on a users' desktop for only their use.

The University community has a right to expect the integrity of fully maximizing, data resources, data protection, security and accessibility as a part of quality data consistency.

Currently, CAU is at risk due to the following eight performance gaps, *to name a few*, that could potentially cost up to 3 million dollars:

1. Unable to obtain appropriate access to the applicable Banner database and integrated applications in a timely manner
2. Inconsistent data between Banner and the integrated/non-integrated applications
3. Data stored in "shadow" systems or on platforms open for potential risk (i.e. hacking)
4. Inappropriate access to system and/or application
5. Changes made in Banner and integrated/non-integrated applications without testing and/or communication
6. Inconsistent formatting in the data
7. Duplicate or incomplete records
8. Minimal to no use of functionality in Banner and integrated/non-integrated applications

The impact to the University due to the aforementioned challenges can potentially cause data breach resulting in expensive reporting fines, lack of compliance and disciplinary sanctions, loss of financial aid or regional accreditation, etc. Below are a few examples:

- Department of Education Integrated Postsecondary Education Data System (IPEDS) requires mandatory reporting for Institutions with Program Participates Agreements. The University can be fined up to \$35,000 for untimely and inaccurate reporting. (See Appendix A) IPEDS Web resource link: <https://surveys.nces.ed.gov/ipeds/ViewContent.aspx?contentId=18>
- SACSCOC requires candid documentation (SACSCOC Institutional Profile) that includes a host of institutional data that must comply with requirements for integrity, timeliness, and accuracy in reporting data. The University will be sanctioned, denied reaffirmation, or removed from membership. (See Appendix B) SACSCOC Web resource manual: <http://www.sacscoc.org/pdf/Resource%20Manual.pdf>
- Data Breach can potentially cost a University up to 3 million dollars. Data such as names, identification, salary, social security numbers, can be at risk due to inappropriate system access and/or weakened system administration. (See Appendix C) Example of a University data breach Web resource: <http://www.lansingstatejournal.com/story/news/local/2016/11/30/msu-estimates-spending-3-million-responding-data-breach/94541962/>
- Violation of institutional Code of Ethical Conduct policy regarding information technology resources, potential transactions being made that are not warranted, inappropriate users having access to confidential

data, inability to foster wise and cost-effective decision making (See Appendix D) University Compliance Office Web resource: <http://www.cau.edu/compliance-office/includes/files/2-4-0-code-of-ethical-conduct.pdf>

The Committee will collaborate with OPAR, ITEC, and OITC to use this project as a platform to ensure data stewardship by doing the following:

- develop new university IT application controls for protection, access, and use of institutional data
- re-implement existing university IT application controls for protection, access, and use of institutional data
- improve the efficiency and effectiveness of regulatory reviews (i.e. internal/external auditing, SACSCOC)
- Improve the quality of the data in which a consistent formatting is observed for seamless integration of data (i.e. Integration of application XX with Banner), reporting (i.e. Dept. of Education/Federal reporting), and research (i.e. data analysis, trend studies)
- Encourage taking advantage of Banner and integrated/non-integrated applications functionalities
- Establish corrective action plans necessary for reconciliation and maintenance of the data
- Establish institutional data integrity plan with an accompanying data dictionary necessary for the employee onboarding, and record of IT application (system and IT control) changes
- Establish Banner and university funded application succession plans to accompany the institutional data integrity plan for employee onboarding.

1.1 Goals and Objectives (Note: Objective Measures are in section 2 of this document)

Goals	Objectives
<p>Establish Institutional Data Integrity plan for Banner, university funded applications, and non-Banner systems.</p>	<p>1. Develop and distribute a template for Banner, university funded applications, and non-Banner systems data stewards.</p> <ul style="list-style-type: none"> - The Committee will work with OITC and Banner (Ellucian) to identify all utilized Banner modules, university funded applications, and non-Banner systems. - The Committee will identify data stewards for all Banner modules, university funded applications, and non-Banner systems. - The Committee will create and distribute a template that will collect the following from data stewards: <ul style="list-style-type: none"> - Banner Module or non-Banner application/systems utilized by the data stewards' department - Data Steward and Data Designee (Backup to Data Steward) - "Superusers" and non- Superusers assigned access privileges, roles and responsibilities, etc. - Catalog of the type of data being stored - Timeframe for when the data is reviewed, maintained, and reconciled (if exist) - Data standards, data definitions, and accountability measures (if exist) - Existing succession plan (if exist) <p>2. Vet all template information and collaborate with data stewards on those elements requiring further feedback or creation of data standards or succession plan.</p> <p>3. Document and make public for all Banner, university funded applications, and non-Banner systems current and future users.</p>

	<ul style="list-style-type: none"> - The Committee will work with OITC, Banner (Ellucian) team, and data stewards regarding the best location to store this document electronically or otherwise (i.e. CAU website).
Improve the quality of institutional data	<ol style="list-style-type: none"> 1. Work with OITC and Banner (Ellucian) team to aid in reducing Banner related challenges. The Committee will seek ways to provide support regarding following: <ul style="list-style-type: none"> - Banner Maintenance (Overhaul) Schedule - Preparation for Banner 9 upgrade - Banner Data scrubbing and reconciliation - Banner Superuser succession plan - Support needed for audit related data recommendations - Future application integrations 2. Create or implement existing data standards to prevent inconsistent data between Banner and university funded integrated and non-integrated applications. 3. Create or implement existing data standards for consistent data formatting and incomplete records.
Bring Banner and university funded applications under affirmative data stewardship	<ol style="list-style-type: none"> 1. Create or implement existing user access controls for Banner. 2. Create or implement existing user access controls for university funded applications.
<p>Fully maximize the functionality of Banner university funded applications</p> <p><i>**Measures for this goal are to be determined with data stewards.</i></p>	<ol style="list-style-type: none"> 1. Identify current "shadow" systems utilized by data stewards. 2. Identify available functionalities in Banner and university funded application that are underutilized. <ul style="list-style-type: none"> - The Committee will work with Banner (Ellucian) team to identify all unused Banner functionality. - The Committee will glean rationale from appropriate data stewards regarding the pros and cons of using shadow systems or non-integrated applications in the place of Banner. 3. Identify ways to utilize Banner functionality. <ul style="list-style-type: none"> - The Committee will work with data stewards and Banner (Ellucian) team to discover ways to maximize use of Banner functionalities.

1.2 Organizational Impacts

Group	Impact to and Participation Required
OITC	50% participation – technical/security support; data standards committee support
Banner (Ellucian)	50% participation - Banner/security support; data standards committee support
OPAR	50% participation – SACS standards and federal reporting requirements support; data standards committee support

Compliance Office	25 % participation – Compliance requirements support; data standards support (training)
CAU	25% participation – other Advisory committee project support

1.3 **Obvious Limitations** (Problems or Issues the project will NOT address even though people think/hope/have asked it might or should)

Group	Impact to and Participation Required
OITC	Limitation in departmental resources (staff); support of data standards committee interrupts the business operations
Banner (Elucian)	Limitation in departmental resources (staff); support of data standards committee interrupts the business operations
CAU	Lack of knowledge by CAU about the Data Standards committee existence; Inadequate project participation (support of data standards committee interrupts the business operations); Compressed testing and UAT

1.3.1 **Plan to Monitor and Mitigate Risk**

The Project Manager along with The Committee will contribute to effective project risk management by ensuring that project participants will effectively carry out the actions listed below:

- Develop risk mitigation plan for each project and update the plan as the project progress
- Start the risk management process early in the project life cycle
- Require project participants to report on the status of their activities and progress of project risk at every project review meeting
- Effectively communicate progress and changes to project risks and mitigation plans to ITEC
- Evaluate project risks and risk responses periodically during the project life cycle
- Follow through with mitigation actions until risks are acceptable

2 MEASURABLE PROJECT OBJECTIVES AND RELATED SUCCESS CRITERIA

Goals	Objectives and Measures
Establish Institutional Data Integrity plan for Banner, university funded applications, and non-Banner systems.	<p>Measure #1: Develop an Institutional Data Integrity plan template to distribute to applicable data stewards.</p> <p>Measure #2: 100% (x out of x)* of data stewards will submit their completed plan template to the Data Standards committee by XX 2018 or the close of their project.</p> <p>Measure #3: The Data Standards Committee will review and approve 100% (x out of x)* completed plans by XX 2018 or the close of their project.</p> <p>Measure #4: 100% (x out of x)* data stewards will participate in all mandatory Data Standards focus group (as provided by either the Data Standards Committee).</p>
Improve the quality of institutional data	<p>Measure #1: 100% (x out of x)* applications will undergo a review of their application data inconsistencies at the start of Fall and Spring semesters.</p> <p>Measure #2: 100% (x out of x)* of units will correct inconsistencies before the start of Fall and Spring semesters.</p>
Bring Banner and university funded applications under affirmative data stewardship	<p>Measure #1: 90% (x out of x)* of data stewards will submit quarterly review of user access privileges.</p> <p>Measure #2: 100% (x out of x)* of data stewards will undergo an annual review of the applicable institutional data integrity plan.</p> <p>Measure #3: 100% (x out of x)* data stewards will participate in all mandatory Data Standards training (as provided by either the Data Standards Committee in conjunction with the University Compliance Office and/or OITC).</p>

*To determine the Criteria for success for each performance measure, each measure will be evaluated based on a percentage of on-time submission and/or completion of each task. Therefore, each performance measure will include (x out of x) which determine the percentage.

3 PROJECT REQUIREMENTS PHASES (High Level) – Applicable to any project charter

Initiation	The Committee must review all project charters submitted by the other Advisory committees to determine how best to
------------	--

(Trigger Customer: other Advisory Committee chair)	lend support (i.e. creating or implementing an existing data standard, sharing knowledge of SACS standard or federal reporting requirement, etc.)
Planning (Main department: The Committee)	Planning phase will be a collaborative effort between The Committee and the other Advisory committee chair; The Committee will: Determine all users that could be affected by the request; Identify all risks associated with project request and develop a risk mitigation plan; Determine steps and approvals needed to implement all activities to support the other Advisory committees' project will be determined.
Execution (Support Group/Execution Partners: OPAR, OITC, Banner (Ellucian) (Approval Partners: ITEC and/or data steward and/or Banner (Ellucian) for approvals)	<p>If project involves knowledge of SACS standards, Compliance, or Federal reporting requirement:</p> <p>The Committee will collaborate with OPAR and/or the Compliance office to provide documentation and impacts of the standard, audit, or requirement.</p> <p>If project involves a data, application, or system change:</p> <p>The Committee will collaborate with OPAR and/or the Compliance office to provide documentation and impacts of the standard, audit, or requirement that relates to the change.</p> <p>The Committee will request approval from ITEC and/or data stewards for all activities necessary for system or application modification; if testing is involved, The Committee will work with Banner (Ellucian) team and/or the appropriate data steward to either obtain appropriate access to the Testing environment or submit a testing request to the data steward to test the modification to the system or application.</p> <p>The Committee will provide all testing results and outcome to the other Advisory committee chair.</p>
Closure (Customer: other Advisory Committee chair)	The Committee must work with the appropriate data steward to notify all users affected by the modification. The Institutional Data Integrity Plan will be updated accordingly to reflect all related information regarding the modification.

*Requirements will be based on the project charters submitted by other Advisory committee.

3.1 Departmental or Contractor Statements of Work (SOW)

TITLE of the SOW	Owner/Prime	Internal/External	Sequence (Phase in Project Lifecycle)
Trigger – provide the project charter and request details	Other Advisory Committee Chair	Internal	Initial Phase

Planning - planning to determine all users affected, potential risks, develop a risk mitigation plan, steps and approvals needed to implement all activities	The Committee	Internal	Planning Phase
Execution – execution of all project assigned activities	OITC, OPAR, Compliance, CAU areas (Registrar, Admissions, etc.	Internal/possibly external depending outside source is suggested by project team	Execution Phase
Closure - notify all users affected by the modification and update Institutional Data Integrity Plan to reflect all related modification information.	The Committee, in conjunction with other Advisory Committee	Internal	Closure Phase

3.3 Summary of Milestones with Due Dates & Estimated Costs

Project Milestone	Date Estimate	Deliverable(s) Included	Preliminary Cost Estimate
Project Planning and Execution Staffing and/or Temp Help	Will be determined by project charter	Yes	See Budget Template
Project Planning and Execution Banner (Ellucian) Consultant	Will be determined by project charter	Yes	See Budget Template

4 TEAM/HUMAN RESOURCES:

Core Project Time: *(Planning Team)*

Project Team Role	Project Team Member(s)	Responsibilities	Percent of Time Available
OPAR	Tarji Kinsey	Project Manager	25%
Banner (Ellucian)	Ayanna Overall	Banner Representative; Data Standards Committee Chair	25%
Data Standards Committee	Ayanna Overall Tarji Kinsey	Team Member	25%

	Lorri Sadler-Rice Cynthia Williams Susan Gibson Leighton O'Sullivan Shemitria Smith James Stotts Latonia Thompson Jessie Wilson Maggie Yan Rodney Fowlkes		
OITC	Rodney Fowlkes Jessie Wilson	Team Members	25%
OPAR	Dr. Narendra Patel Dr. Lauren Lopez	Team Members	25%

Full Project Team: (Execution Team)

Project Team Role	Project Team Member(s)	Responsibilities	Percent of Time Available
OPAR	Tarji Kinsey	Project Manager	25%
Banner (Ellucian)	Ayanna Overall	Banner Representative; Data Standards Committee Chair	25%
Data Standards Committee	Ayanna Overall Tarji Kinsey Lorri Sadler-Rice Cynthia Williams Susan Gibson Leighton O'Sullivan Shemitria Smith James Stotts Latonia Thompson Jessie Wilson Maggie Yan Rodney Fowlkes	Team Member	25%
OITC	Rodney Fowlkes Jessie Wilson	Team Members	25%
OPAR	Dr. Narendra Patel Maggie Yan Dr. Lauren Lopez	Team Members	25%
Compliance	Robert Clark	Team Member	25%
Other Advisory Committee	Chair	Project Manager	25%

5 PROJECT APPROVAL REQUIREMENTS

	Success Criteria	Date Complete	Signed Off by:
--	------------------	---------------	----------------

1	Project support for Audit	Will be determined by project charter	Audit Committee
2	Project support re: Data Standards	Will be determined by project charter	Department managers, OITC, OPAR, Banner (Ellucian)
3	Project support for Compliance	Will be determined by project charter	Compliance office, OPAR, OITC

6 SUMMARY PROJECT BUDGET (Included in CAU Budget Submission Template)

#	Phase	Amount
1	Planning - Staffing and/or Temp Help; Banner (Ellucian) SME or Consultant; Training	\$21,750.00
2	Execution - Staffing and/or Temp Help; Banner (Ellucian) SME or Consultant; Training	\$21,750.00
	Estimated Total Cost	\$43,500

Note: 25% is the estimated need of time per month that a person will be to work on those activities, not a part of their normal job responsibilities, during both Planning and Execution phases of the project. Two people will be needed from applicable units. Example: If a project charter involves OPAR, two people from OPAR will be needed 25% of the time per month to collaborate with the Committee during the Execution phase (Estimated cost: 35 hours per month @ \$50 an hr = \$1750 x 2pp = \$3500).

7 HIGH LEVEL PROJECT RISKS


Project Risks

#	Risk Area	Likelihood	Risk Owner	Project Impact-Mitigation Plan
1	Lack of knowledge about the Data Standards committees existence	Medium	Executive Sponsor/ITEC	Emphasize the importance of the Data Standards Committee and its charge
2	Inadequate project participation (support of data standards)	High	Department Managers OITC	Emphasize this is an opportunity to improve the quality of institutional data

	committee interrupts the business operations)		Banner (Ellucian)	used of university decision-making and reporting. Reiterate this is an opportunity to better protect and access institutional data
3	Compressed testing and UAT	High	Data Stewards	Participate in the testing activities Monitor testing activities by requesting the status and progress of testing activities


8 APPROVALS

Prepared by



 Project Manager

Approved by



Project Sponsor (Advisory Council Member Sponsor)

 Executive Sponsor

 Customer

Clark Atlanta University		
Data Stewardship Project		
Budget Detail		
	Estimated	Frequency
Planning Phase		
A. Staffing and/or Temp Help; Banner (Ellucian) SME or Consultant	\$15,750	Monthly
OITC - 2 people @ \$50 hr for 35hrs	\$3,500	
Banner CAU SME - 1 person @ \$50 hr for 35hrs	\$1,750	
OPAR - 2 people @ \$50 hr for 35hrs	\$3,500	
Faculty Advisor - 2 people @ \$50 hr for 35hrs	\$3,500	
CAU representative applicable to the project (i.e. Registrar, Financial Aid, Admissions, etc.) - 2 people @ \$50 hr for 35hrs	\$3,500	
B. Training - Data Standards/Integrity Conference	\$6,000	Annual
Data Standards Committee to attend training- 3 people @ \$2,000 for conference cost, flight, hotel, per diem	\$6,000	
Total Estimated Planning Phase Cost	\$21,750	
Execution Phase		
A. Staffing and/or Temp Help; Banner (Ellucian) SME or Consultant	\$15,750	Monthly
OITC - 2 people @ \$50 hr for 35hrs	\$3,500	
Banner CAU SME - 1 person @ \$50 hr for 35hrs	\$1,750	
OPAR - 2 people @ \$50 hr for 35hrs	\$3,500	
Faculty Advisor - 2 people @ \$50 hr for 35hrs	\$3,500	
CAU representative applicable to the project (i.e. Registrar, Financial Aid, Admissions, etc.) - 2 people @ \$50 hr for 35hrs	\$3,500	
B. Training - Data Standards/Integrity Conference	\$6,000	Annual
Data Standards Committee to attend training - 3 people @ \$2,000 for conference cost, flight, hotel, per diem	\$6,000	
Total Estimated Execution Phase Cost	\$21,750	
Total Estimated Cost of Project	\$43, 500	

Note: Estimated cost are based on those activities that are not apart of the CAU employees normal job description/role and responsibilities.

NCES National Center for Education Statistics

Statutory Requirements for Reporting IPEDS Data

General Mandate

NCES is authorized by law under the Section 153 of the Education Sciences Reform Act of 2002 (P.L. 107-279). Accordingly, NCES "shall collect, report, analyze, and disseminate statistical data related to education in the United States and in other nations, including -

- collecting, acquiring, compiling (where appropriate, on a state by state basis), and disseminating full and complete statistics on the condition and progress of education, at the pre-school, elementary, secondary, and postsecondary levels in the United States, ...;
- conducting and publishing reports and analyses of the meaning and significance of such statistics;
- collecting, analyzing, cross-tabulating, and reporting, to the extent feasible, so as to provide information by gender, race, ...; and
- assisting public and private educational agencies, organizations, and institutions in improving and automating statistical and data collection activities..."

Mandatory Reporting for Institutions with Program Participation Agreements

The completion of all IPEDS surveys, in a timely and accurate manner, is mandatory for all institutions that participate in or are applicants for participation in any Federal financial assistance program authorized by Title IV of the Higher Education Act (HEA) of 1965, as amended. The completion of the surveys is mandated by 20 USC 1094, Section 487(a)(17) and 34 CFR 668.14(b)(19).

The Department of Education relies on postsecondary institutions to accurately report data to IPEDS, and nearly all institutions do. Institutions themselves sometimes identify misreporting issues and work with ED to correct those problems without the need for further action by the Department. The Department is concerned about any instances of intentional or significant misreporting. Under these circumstances, the Office of Federal Student Aid may take administrative action to appropriately address the issue.

Title IV, HEA program regulations 34 CFR 668.84, 668.85, and 668.86 provide that the Department may initiate a fine action or other administrative action, such as a limitation, suspension, or termination of eligibility to participate in the Title IV, HEA programs, against institutions that do not comply with the requirement to complete and submit their IPEDS surveys. The regulations permit a fine of up to \$35,000 for each violation of any provision of Title IV, or any regulation or agreement implementing that Title. In determining the amount of a fine, the Secretary considers both the gravity of the offense and the size of the institution (34 CFR 668.92(a)).

Each year, the Office of Federal Student Aid issues fine notices to institutions for not completing their IPEDS surveys in a complete and accurate manner within the required timeframes. Other institutions are sent warning letters. According to the Office of Federal Student Aid, an institution's failure to accurately complete and submit these surveys is a serious violation of its obligations under the Higher Education Act, and appropriate action will be taken.

Vocational Education Data

IPEDS responds to certain of the requirements pursuant to Section 421(a)(1) of the Carl D. Perkins Vocational Education Act. The data related to vocational programs and program completions are collected from postsecondary institutions known to provide occupationally specific vocational education.¹

Data on Race/Ethnicity and Gender of Students

The collection and reporting of race/ethnicity and gender data on students and completers are mandatory for all institutions which receive, are applicants for, or expect to be applicants for Federal financial assistance as defined in the Department of Education (ED) regulations implementing Title VI of the Civil Rights Act of 1964 (34 CFR 100), or defined in any ED regulation implementing Title IX of the Education Amendments of 1972 (34 CFR 106). The collection of race/ethnicity and gender data in vocational programs is mandated by Section 421(a)(1) of the Carl D. Perkins Vocational Education Act.

Data on Race/Ethnicity and Gender of Staff

The collection and reporting of race/ethnicity and gender data on the Human Resources (HR) component are mandatory for all institutions which receive, are applicants for, or expect to be applicants for Federal financial assistance as defined in the Department of Education (ED) regulations implementing Title VI of the Civil Rights Act of 1964 (34 CFR 100). The collection of these data is also mandated by P.L. 88-352, Title VII of the Civil Rights Act of 1964, as amended by the Equal Employment Opportunity Act of 1972 (29 CFR 1602, subparts O, P, and Q). Institutions with 15 or more full-time employees are required to respond to the IPEDS Human Resources component under this mandate.

Student Right-to-Know

Sections 668.41, 668.45, and 668.48 of the Student Assistance General Provision (34 CFR 668) were amended to implement the Student Right-to-Know Act, as amended by the Higher Education Amendments of 1991 and further by the Higher Education Technical Amendments of 1993 and 1999. The final regulations require an institution that participates in any student financial assistance program under Title IV of the Higher Education Act of 1965, as amended, to disclose information about graduation or completion rates to current and prospective students. The final regulations also require such institutions that also award athletically related student aid to provide certain types of data regarding the institution's student population, and the graduation or completion rates of categories of student-athletes, to potential athletes, their parents, coaches, and counselors.

Consumer Information

Section 101 of the Higher Education amendments of 1965 (P.L. 105-244) requires that NCES collect the following information about undergraduate students from institutions of higher education: tuition and fees, cost of attendance, the average amount of financial assistance received by type of aid, and the number of students receiving each type.

Section 132 of the Higher Education Act of 1965 (P.L. 110-315), as amended, requires that NCES make the following consumer information about postsecondary institutions available on the [College Navigator](#) college search web site: the institution's mission statement; a link to the institution's website that provides, in an easily accessible manner, information on student activities, services for individuals with disabilities, career and placement services, and policies on transfer of credit; admissions rates and test scores; enrollment by race and ethnicity, gender, enrollment status, and residency; number of transfer students; students registered with the disability office; retention rates; graduation rates within normal time of program completion and 150% and 200% of normal time; number of certificates and degrees awarded, and programs with the highest number of awards; student-to-faculty ratio and number of faculty and graduate assistants; cost of attendance and availability of alternative tuition plans; average grant aid and loans, and number of students receiving such aid, by type; total grant aid to undergraduates; number of students receiving Pell Grants; three years of tuition and fees and average net price data; three years of average net price disaggregated by income; a multi-year tuition calculator; College Affordability Lists and reports; Title IV cohort default rate; and campus safety information. State spending charts and a link to Bureau of Labor Statistics information on starting salaries are also required.

¹Institutions providing vocational/occupational programs are identified through responses to the Institutional Characteristics (IC) survey and the Completions (C) survey.



1.1 The institution operates with integrity in all matters.

(Note: This principle is not addressed by the institution in its Compliance Certification.)

Rationale and Notes

Institutional integrity serves as the foundation of the relationship between the Commission on Colleges and its member and candidate institutions. This fundamental philosophy is reflected in the *Principles of Accreditation* as follows:

“Integrity, essential to the purpose of higher education, functions as the basic contract defining the relationship between the Commission and each of its member and candidate institutions. It is a relationship in which all parties agree to deal honestly and openly with their constituencies and with one another. Without this commitment, no relationship can exist or be sustained between the Commission and its accredited and candidate institutions.”
(Page 13)

As a condition of candidacy or membership with the Commission on Colleges, the institution agrees to document its compliance with the requirements of the *Principles of Accreditation*; to comply with Commission requests, directives, decisions and policies; and to make complete, accurate and honest disclosure to the Commission.

The Commission’s policy, “Sanctions, Denial of Reaffirmation, and Removal from Membership,” states that the Commission on Colleges requires a member institution to be in compliance with the Core Requirements, Comprehensive Standards, Federal Requirements, Commission policies and procedures, and to provide information as requested by the Commission in order to maintain membership and accreditation. The policy also states:

“Failure to respond appropriately to Commission decisions and requests or to make complete, accurate, and honest disclosure is sufficient reason, in and of itself, for the Commission to impose a sanction, including the denial or revocation of candidacy or accreditation.” (Page 1)

In order to comply with these requirements for integrity and accuracy in reporting in its relationships with the Commission, the chief executive officer and accreditation liaison must review and ensure the accuracy and integrity of materials submitted by the institution, such as the Compliance Certification and Quality Enhancement Plan. In addition, an institution shall meet the following expectations:

1. Ensure that all documents submitted to the Commission are completely candid, providing all pertinent information whether complimentary or otherwise. With due regard for the rights of individual privacy, every institution applying for candidacy, extension of candidacy, accreditation, or reaffirmation of accreditation, as well as every candidate and accredited institution, provide the Commission with access to all parts of their operations, and with complete and accurate information about the institution’s affairs, including reports of other accrediting, licensing, and auditing agencies.
2. Respond in a timely manner to requests by the Commission for submission of dues, fees, reports, or other information.
3. Ensure that other information submitted to the Commission (such as that provided in the annual institutional profile, institutional responses to visiting committee reports, and monitoring reports) is complete, accurate, and current.

4. Cooperate with the Commission in preparation for visits, receive visiting committees in a spirit of collegiality, and comply with the Commission's requests for acceptable reports and self-analyses.
5. Report substantive changes, including the initiation of new programs or sites outside the region or within the region, in accordance with the Commission policy on Substantive Change.
6. Report accurately to the public its status and relationship with the Commission.
7. Provide counsel and advice to the Commission, and agree to have its faculty and administrators serve, within reason, on visiting teams and on Commission committees.
8. Provide the Commission or its representatives with information requested and maintain openness and cooperation during evaluations, enabling evaluators to perform their duties with maximum efficiency and effectiveness.
9. Maintain current knowledge and understanding of both the product and process of accreditation/reaffirmation and be able to address/complete all requirements of the SACSCOC in a timely and accurate manner.

The Commission accredits institutions, not individuals. Therefore, any individual who reports to the Commission on behalf of an institution—either by virtue of his or her office or as delegated by the chief executive officer of the institution—obligates the institution in all matters regarding institutional integrity.

Reference to Commission Documents, if applicable

"Integrity and Accuracy in Institutional Representation"

Cross References to other related Standards/Requirements, if applicable

Applies to compliance with all standards/requirements and policies

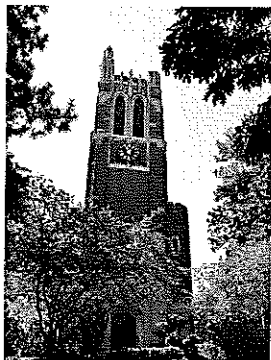
Appendix C

New Year Sale Celebrate Together The New Year

SUBSCRIBE (HTTP://OFFERS.LANSINGSTATEJOURI GPS-SOURCE=BENBDEC&UTM_MEDIUM=N, EXCHANGE&UTM_CAMPAIGN=NEWYI

Data breach could cost \$3 million, Michigan State says

By RJ Wolcott, Lansing State Journal Published 7:07 a.m. ET Nov. 30, 2016 | Updated 12:37 p.m. ET Nov. 30, 2016



(Photo: LSJ file photo)

EAST LANSING - Whoever hacked into a Michigan State University database earlier this month "found the Holy Grail," according to one security expert.

Names and MSU identification numbers were exposed along with social security numbers, which are extremely valuable to criminals, said Paul Stephens, director of policy and advocacy for Privacy Rights Clearinghouse (<https://www.privacyrights.org/>).

Armed with social security numbers, a criminal could open up new credit cards or file someone's taxes and collect their refund. And unlike having a credit card number exposed, consumers can't simply call their bank and have the account closed, Stephens said.

Between providing identity protection and enhancing its security systems, MSU estimates that it will spend \$3 million in response to the attack.

What should you do if you're part of MSU data breach?

(<http://www.freep.com/story/money/personal-finance/susan-tomp/or/2016/11/23/michigan-state-data-breach-tips/94235440/>)

The potential for identity theft underscores why institutions like MSU shouldn't hold onto these records for more than a couple years after someone leaves, Stephens added.

Ad

3 Bureaus Credit Scores

www.nationalcreditrepo...



VISIT SITE

"There's no need to maintain certain data elements," Stephens said. "And MSU shouldn't have maintained social security numbers."

MSU spokesman Jason Cody defended MSU's record keeping, saying the university needs the records because it maintains "ongoing relationships with members of our community long after they leave us."

MSU also keeps extensive records for current and past employees who collect benefits through MSU, Cody added.

An email from the alleged hacker seeking money arrived on Nov. 13, alerting the university to the data breach, Cody said. Some 400,000 records of current and former students and staff were on the exposed database. MSU first announced the breach and began alerting those affected five days after finding out about the attack and about an hour before most banks close for the week.

New Year Sale. Celebrate Together The New Year

SUBSCRIBE
HTTP://WWW.LANSINGSTATEJOURNAL.COM/...
GPS:
SOURCE=BENBDEC&UTM_MEDIUM=N,
EXCHANGE&UTM_CAMPAIGN=NEWYI

Defending the amount of time between the attack and the alert, Cody said law enforcement officials needed to be contacted and the cause of the attack needed to be identified to prevent further attacks. MSU's timeframe "wasn't particularly egregious," according to Stephens.

While MSU may review its data policies in response to the breach, there are no current plans to change what information is kept, Cody said. Forensic experts from MSU, alongside law enforcement, confirmed only 449 of the 400,000 exposed records were accessed.

Stephens cast doubt on that figure.

"If (MSU) couldn't see their database was hacked in the first place, how much confidence can you put in the number of records accessed," he asked, referring to the fact that MSU was notified of the hack by an alleged perpetrator.

MSU officials have signed a contract with AllClear ID (<https://www.allclearid.com/>) to provide identity protection for anyone whose records were on the compromised database.

A recent study funded by IBM (<http://www-03.ibm.com/security/data-breach/>) found the average cost of a data breach for affected organizations is about \$4 million.

More than 5,200 data breaches have been made public since 2005, according to Privacy Rights Clearinghouse (<https://www.privacyrights.org/data-breaches>), exposing some 900,000,000 records. MSU is targeted, "hundreds of thousands of times" a month by digital attacks, Cody said, from attempted breaches to malware emails.

After the email arrived, MSU immediately contacted law enforcement and began investigating how the breach occurred, Cody said. The database was taken offline within 24 hours. MSU has determined the breach was caused by a piece of licensed software.

Those affected include students who attended MSU between 1991 and 2015 and faculty, staff and students employed by the university between 1970 and Nov. 13.

Despite never working for or attending MSU, Jeff Kussow said he received a letter from MSU saying his records were part of the breach.

"In fact, I've never set foot on the campus and don't recall enrolling in anything they've offered, even online," Kussow wrote in an email.

Applying to graduate school at in the mid-1990s was the only contact Kussow remembers having with MSU.

Cody said there's no reason to believe information from applicants was on the compromised database. A handful of people like Kussow have contacted MSU in the past week after receiving letters despite no connection to MSU. Cody chalked it up to someone having the same name as someone who did attend or work for the university.

MSU began sending out emails and letters about the hack Nov. 18, Cody said. Anyone whose data was comprised is advised to visit msu.edu/datasecurity (<http://msu.edu/datasecurity>) to sign up for identity protection. Those wishing to know if they were affected by the breach or wanting to sign up for identity protection should call 1-855-231-9331.

Stephens advised those affected to sign up for additional credit monitoring and file their taxes early to prevent a criminal from claiming their refund.

In 2014, the University of Maryland took about a day to disclose a data breach that included some 300,000 personal records. That same year, Target waited close to two months to let customers know of a breach that affected millions of customers. Ohio State University took about a month in 2010 to disclose that some 760,000 people had their data exposed and were at risk of identity theft.

Cody said further details about the breach, including where it came from, aren't yet known. A criminal investigation is ongoing.

Contact RJ Wolcott at (517) 377-1026 or rwolcott@lsj.com (<mailto:rwolcott@lsj.com>). Follow him on Twitter [@wolcott](https://twitter.com/WolcottR) (<https://twitter.com/WolcottR>).

Looking for identity protection

For help signing up for identity protection, call 1-855-231-9331 or visit msu.edu/datasecurity/

Policy 2.4.0 Code of Ethical Conduct

Q: While I was on vacation, my supervisor used my computer and accessed some personal information I have stored on the hard drive. What can I do to prevent this kind of “snooping” in the future?

A: An individual’s personal information stored on CAU-owned computer equipment is not confidential. As with personal e-mails, information that is stored or transmitted via CAU’s information systems is not private communication.

Responsible Use of Technology

CAU provides a variety of computing resources including e-mail, Web hosting and Internet connectivity to its employees. These resources are a cost-effective way to conduct business. CAU wants to encourage the responsible use of computer technology by adhering to local, state and federal laws governing computer use. Violations of CAU computing resources include actions such as harmful actions towards minors, threats, harassment, use of obscenity, forgery, unsolicited e-mail, unauthorized access, collection of personal data, reselling services, service interruptions, physical security, copyright and trademark infringement among other things.

Q: I suspect that employees in my office are using their computers to conduct business that violates University policy. What should I do?

A: Report the suspected activities to your supervisor or the Compliance Office. The following information must be provided: the date and time of the alleged activity and a detailed description of the alleged activity.

System Access and Passwords

Attempting to access University computers without specific authorization is prohibited. Any form of tampering, including snooping and hacking, to gain access to computers is a violation of University policy, and carries serious consequences. Employees are required to turn off their computers at the end of the day, and when not in use for an extended period of time. This will help prevent computer security breaches and damage due to power surges. In addition, computer users must take other reasonable precautions to prevent unauthorized access of University computers.

Computer passwords are used to protect your computer, electronic files and other data. External attacks on computers often rely on weak passwords based on personal data and common words. By creating strong alpha numeric passwords you are protecting University data.

For more information on passwords, please see the Information Technology and Communications Operating and Security Policy for Students, Faculty and Staff located on the CAU Web site.

Q: Is it acceptable to share your password when you are in a crunch for time or will be out of the office?

A: No. You should never share your password. If additional passwords are required, follow the procedure established to request access. Individuals who share their passwords are accountable for actions taken under their login.