THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting Agenda

August 7, 2024 - 1:00 p.m. C.T. - Virtual Meeting

1. Opening Remarks – Chancellor Tydings
2. Policy 2.01.00.00 General Education Requirements and Degree Requirements – Reed and Denn
3. New Proposed Guideline G-035, Non-Credit Programs and Proposed Revisions to Policy 9.01.03.00, Advertising – Stewart
4. New Proposed Guideline A-115, Foreign Talent Recruitment Programs – Stewart

Consent Agenda #1

5. Proposed Revisions to 4.02.01.00, Approvals of Agreements and Contracts – Stewart
6. Proposed revisions to Policy 6.04.00.00, Pregnancy, Childbirth, and Related Medical Conditions – Stewart

Consent Agenda #2

7. 1.08.04.00 Personally Identifiable Information Policy - Calisi
8. B-090 Safeguarding Nonpublic Financial Information Guideline - Calisi
9. Digital Identity Authentication Management and Access Control Policy - Calisi

Informational Items

10. Legislative Priorities – McCormick
11. Retirement of Legacy Policy System Effective September 1, 2024 – Stewart
12. Clery Act Compliance Reminder – Stewart
13. Gainful Employment – Button and Tingle
14. Cyber Security Update/Insurance – Fox and Calisi
15. Licensure and Program Accreditation Title IV Compliance – Reed
16. Reimagining the Education Core - Reed and Denn
17. Correctional Education Initiative - Reed, Sewell and Rhae
18. NC-Sara and Title IV Compliance – Lopez and Button
19. Workforce Convening Update – Sisk and Adams
20. Other Business and Adjournment – Chancellor Tydings

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT:	Policy 2.01.00.00 General Education Requirements and Degree Requirements
PRESENTER:	Vice Chancellor Jothany Reed Associate Vice Chancellor Robert Denn
ACTION REQUIRED:	Requires Vote

Summary:

The review process for Policy 2.01.00.00 began in March 2024 with the General Education Core Steering Committee and was presented for first reading at the April 2024 Joint Academic Affairs/Student Affairs and Faculty Sub-council meetings. The policy was posted for a one-month, open comment period for all sub-council members, and suggested revisions were incorporated into the proposed final document. Those revisions are grouped into the following:

1. Reference the 2025 TBR Core framework document. (§I.A)
2. Remove sections pertaining to university governance and degrees. (§II. A)
3. Remove clauses more appropriate for other policies.
   2.00.01.06 Articulation and Transfer (§II.B.3)
   2.03.00.00 Admission at the Community Colleges (§IV)
   2.03.00.02 Community College Learning Support (§II.C)
4. Remove inactive links. (§I.C)
5. Specify degrees with special distribution requirements. (§I.D)
6. Delete defunct deficiency thresholds. (§II.D.)
7. Include Core course approval process. (§III)
8. General language cleanup/clarification/organization.

The proposed revised policy passed unanimously through the Joint Academic Affairs/Student Affairs Sub-council and the Faculty Sub-council during their July 2024 meetings. Pending approval by the Presidents Council, this policy is scheduled to go before the Board at its September 2024 quarterly meeting.

Current, mark-up, and clean copies of the proposed revised policy are enclosed.

2.01.00.00 General Education Requirements and Degree Requirements

2.01.00.00 General Education Core and Degree Requirements

Policy/Guideline Area

Academic Policies

Applicable Division

Community Colleges

Purpose

The purpose of this policy is to specify the ~~common~~ general education core requirements for degrees conferred by community colleges ~~at the lower-division, for institutions governed by the Tennessee Board of Regents~~.

Policy/Guideline

I. General Education Core Requirements

A. E~~ffective Fall Semester 2004, e~~ach ~~institution in the State University and c~~Community c~~C~~ollege ~~System of Tennessee (hereafter identified as the Tennessee Board of Regents System)~~ will subscribe to the~~common~~ general education core requirements stated in the policy sections below and as published in the TBR Core framework document, effective fall semester 2025 (see exhibit A).~~at the lower-division~~.

B. These requirements consist of forty-one (41) semester hours in the following subject categories and are required for completion of the Associate of Arts (A.A.), Associate of Science (A.S.), Associate of Science in Teaching (A.S.T.), and Associate of Fine Arts (A.F.A.)~~all baccalaureate degrees~~.

1. Communication: 9 semester hours

a. Six (6) semester hours of English composition and three (3) semester hours in English oral presentational communication are required.

2. Humanities and/or Fine Arts: 9 semester hours

a. One course must be in literature.

3. Social/Behavioral Sciences: 6 semester hours

4. History: 6 semester hours

a. ~~Students who lack the required one unit (one year) of American history from high school as an admissions requirement must complete six (6) semester hours of American History or three (3) semester hours of American History and three (3) semester hours of Tennessee History to fulfill the history requirement in general education. Otherwise, students may choose from among the history courses approved at a particular institution to fulfill the six semester hour requirement in history.~~

5. Natural Sciences: 8 semester hours

6. Mathematics: 3 semester hours

C. ~~Total 41 semester hours.~~

C~~D~~. Courses specified as meeting general education requirements are published in the catalog of each institution. ~~and may be viewed at the following TBR link. https://www.tbr.edu/academics/transfer-and-articulation~~

E. ~~Students pursuing a Bachelor of Arts degree shall be required to demonstrate proficiency in a foreign language equivalent to completion of two years of college level work.~~

F. ~~Students pursuing an Associate of Arts degree shall be required to demonstrate proficiency in a foreign language equivalent to completion of one year of college level work.~~

D.~~G~~. Students pursuing an~~s~~ Associate~~s~~ of Fine Arts degree in Music as a Tennessee Transfer Pathway will complete all of the required g~~G~~eneral c~~E~~ducation hours in Section B. above except for six hours of the humanities requirement, including one course in literature, which must be completed at a university upon transfer. ~~Total 35 hours.~~

II. ~~Undergraduate~~ Degree Requirements and Provisions

A. ~~All baccalaureate degrees offered by institutions in the Tennessee Board of Regents System shall require a maximum of 120 semester hours except in certain degree programs in which approval to exceed the~~

~~maximum has been granted. The programs approved as exceptions to the maximum are identified in institutional catalogs.~~

B.A. ~~–~~All Aassociate of Aarts and Aassociate of Sscience degrees offered by institutions in the Tennessee Board of Regents System shall be designated on the THEC Academic Program inventory as University Parallel degrees and require a maximum of 60 semester hours except in certain degree programs in which approval to exceed the maximum has been granted. The programs approved as exceptions to the maximum are identified in institutional catalogs. For students who complete a Tennessee Transfer Pathway, the corresponding Aassociate of Aarts, ~~or~~ Aassociate of Sscience, or Aassociate of Ffine Aarts degree shall include the title of the pathway in the catalog and on the diploma.

C. ~~Credit hours earned in remedial, developmental or learning support courses are institutional credit; they are not applicable to credit hours required for any certificate, associate, or baccalaureate degree.~~

D. ~~College courses taken to address course deficiencies in high school preparation and to meet minimum university admission requirements effective fall 1989 may be used concurrently to satisfy general education requirements specified above with the exception of foreign language.~~

B. Students pursuing an Associate of Arts degree shall be required to demonstrate proficiency in a foreign language equivalent to completing of one year of college-level work.

~~E. Relative to removing course deficiencies in foreign language, the following provisions apply:~~

~~1. Students who pursue programs leading to the Associate of Science or Bachelor of Science degrees may apply foreign language courses taken to remove the deficiencies as electives, if appropriate, or otherwise as add-on hours.~~

~~2. Students who pursue programs leading to the Associate of Arts and Bachelor of Arts degrees may apply foreign language courses taken to remove deficiencies toward fulfillment of degree requirements.~~

C. The Associate of Applied Science (A.A.S.) degree is not generally designed to transfer to baccalaureate programs without the creation of specific articulation agreements; however, a general education component is required.

Formatted: Indent: Left: 0.5", Hanging: 0.5"

D. The following distribution of general education core courses is required for the A.A.S. degree in all community colleges within the Tennessee Board of Regents System:

1. English Composition: 3 semester hours

2. *Humanities and/or Fine Arts: 3 semester hours

3. *Social/Behavioral Sciences: 3 semester hours

4. *Natural Science/Mathematics: 3-4 semester hours

5.. One additional course from the categories of Communication, Humanities and/or Fine Arts, Social/Behavioral Sciences, or Natural Science/Mathematics 3-4 semester hours

E. Total 15-17 semester hours

F. *Specific courses satisfying these requirements must be the same courses that satisfy the general education core requirement for the Associate of Arts or Associate of Science degrees.

III. Core Course Approval

A. Each community college will list its general education core courses in its catalog and on its website where appropriate.
B. All core courses must be approved by the systemwide Core Review Committee.
C. The Core Review Committee will include one representative from each community college as appointed by its Chief Academic Officer.
D. The Core Review Committee may include one representative from each of the six locally governed TN public universities and one from the UT system.

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Indent at: 1.25"

IV~~II~~. Transfer Provisions of the General Education Core and ~~Tennessee Transfer Pathway Courses~~

~~A.~~ ~~Students who complete the Associate of Arts or Associate of Science or Associate of Science in Teaching degree and transfer to a university within the Tennessee Board of Regents System will have satisfied all lower-division general education requirements.~~

A.~~B~~. ~~University to university transfer students and~~ Ccommunity college students who do not complete the Associate of Arts, ~~or~~ Associate of Science, ~~or~~ Associate of Science in Teaching, or Associate of Fine Arts degree and transfer to another community college ~~institution~~ within the

Tennessee Board of Regents System but who complete blocks of subject categories will have satisfied the general education requirements for the categories of note.

1. For example, if the eight (8) semester hours of natural sciences are completed, then this block of the general education requirement is fulfilled upon transfer to another community college ~~institution~~ within the Tennessee Board of Regents System.

2. When a subject category is incomplete, a course by-course evaluation will be conducted, and the student will be subject to specific requirements of the receiving institution.

3. ~~If a student is following a Tennessee Transfer Pathway, all courses contained within the curriculum of that pathway completed by the student prior to transfer shall be accepted by the institution and be applied either to the general education requirement or area of emphasis requirement as listed in that Tennessee Transfer Pathway.~~

C. ~~Institutional/departmental requirements of the grade of "C" will be honored.~~

~~1. If credit is granted for a course with the grade of "D," any specific requirements for the grade of "C" by the receiving institution will be enforced, except as provided in Section B of Calculation of Grade Point Averages (GPAs) for Courses Transferred and Related Applications.~~

Formatted: Indent: Left: 0.5"

D. ~~In certain majors, specific courses must also be taken in general education.~~

~~1. It is important that students and advisors be aware of any major requirements that must be fulfilled under lower-division general education.~~

Formatted: Indent: Left: 0.5"

~~2. In cases where specific courses are required as a part of general education for certain majors, the student is responsible for enrolling in the correct courses.~~

~~3. Failure to fulfill specific major requirements in lower-division general education may result in the need to complete additional courses.~~

IV. ~~Calculation of Grade Point Averages (GPAs) for all Courses Transferred and Related Applications~~

~~A. Upon receiving courses for transfer, the receiving institution will exclude grades in the calculation of Grade Point Averages (GPAs).~~

Formatted: Indent: Left: 0"

1. Credit will be given for all courses in which passing grades are achieved, including the grade of D.

2. All grades, including F's, W's, etc., must be included on the transfer record.

3. The entire record of transfer students will be considered for eligibility of admission into programs that require attainment of specific grade point averages or where external entities stipulate consideration of the entire student record.

B. Specific application regarding the grade of D pertains as follows:

1. Community college students who complete approved Tennessee Transfer Pathways (TTPs) or parts thereof, the grade of D will be honored and affected courses will not be subject to repetition, except in certain cases where requirements stipulate specific courses must be achieved with a grade of C (2.0) or higher.

2. In routes of transfer outside the TTPs, institutional practices regarding the applicability of the grade of D will be honored.

C. Institutions will follow prescribed state practices in evaluating continuing eligibility for the Tennessee Lottery Scholarship Program, which requires inclusion of calculating the cumulative GPA on all courses taken after graduation from high school.

D. Institutions have the prerogative to develop criteria for honors designations.

E. In cases where a student repeats a course at another institution, the receiving institution should utilize its own repeat policy to exclude the grade/credit originally earned.

F. The provisions noted above will be effective for course work presented for transfer to enroll in summer 2015 and thereafter.

IV. General Education Requirements for the Associate of Applied Science Degree

A. The Associate of Applied Science (A.A.S.) degree is not designed to transfer to baccalaureate programs; however, a general education component is required.

B. The following distribution of general education courses is required for the A.A.S. degree in all community colleges within the Tennessee Board of Regents System.

1. English Composition: 3 semester hours

2. *Humanities and/or Fine Arts: 3 semester hours

Formatted: Indent: Left: 0", Hanging: 0.44"

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0", Hanging: 0.44"

Formatted: Indent: Left: 0", First line: 0"

~~3. *Social/Behavioral Sciences: 3 semester hours~~

~~4. *Natural Science/Mathematics: 3 semester hours~~

~~a. One additional course from the categories of Communication, Humanities and/or Fine Arts, Social/Behavioral Sciences, or Natural Science/Mathematics 3-4 semester hours~~

~~C. Total 15-17 semester hours~~ Formatted: Indent: First line: 0"

~~D. *Specific courses satisfying these requirements must be the same courses that satisfy the general education requirement for the Associate of Arts, Associate of Science, or baccalaureate degrees.~~ Formatted: Indent: Left: 0", First line: 0"

VI. ~~Graduate~~

~~A. Graduate Degree Requirements and Provisions~~ Formatted: Indent: First line: 0"

~~1. Graduate degree requirements vary by discipline and level. Generally, master and doctoral programs require a 3.0 GPA or higher for graduation as stated by the institution.~~ Formatted: Indent: Left: 0", First line: 0"

~~B. Transfer Provision for Graduate Courses~~ Formatted: Indent: First line: 0"

~~1. Transfer credit provisions are set by the institutions in keeping with best practice guidelines. As such, transfer of graduate credit is limited in a number of areas.~~ Formatted: Indent: Left: 0", First line: 0"

~~a. For example,~~

~~(1) the number of hours that may be transferred,~~

~~(2) in equivalency of requirements,~~

~~(3) the procedures for acceptance of graduate transfer credits,~~

~~(4) the period in which courses may be taken and time limits on graduate work varies by institution,~~

~~(5) department and academic program.~~

~~2. In general, courses are eligible for transfer if the grade earned is a "B" or better.~~

Sources

Authority

T.C.A. § 49-8-203; THEC; SACS

Exhibit

2025 TBR Core Model

History

TBR Meetings, June 25, 1976; June 25, 1982; March 20, 1987; June 24, 1988; December 5, 1997; June 29, 2004; September 24, 2004; March 27, 2008; TBR Board Meeting September 25, 2009. TBR Board Meeting, December 2, 2010; September 21, 2012; December 21, 2014 (Removed language in Section I.D. ~~referring~~referring to finding the course information on the TBR and/or Policies & Guideline website. This information will now be on the individual institution's website.); (Added a new link for pathways information.) TBR Meeting March 30, 2016; Revised at Board Meeting June 20, 2019.

2.01.00.00 General Education Requirements and Degree Requirements

2.01.00.00 General Education Core and Degree Requirements

Policy/Guideline Area

Academic Policies

Applicable Division

Community Colleges

Purpose

The purpose of this policy is to specify the general education core requirements for degrees conferred by community colleges.

Policy/Guideline

I. General Education Core Requirements

A. Each community college will subscribe to the general education core requirements stated in the policy sections below and as published in the TBR Core framework document, effective fall semester 2025 (see exhibit A).

B. These requirements consist of forty-one (41) semester hours in the following subject categories and are required for completion of the Associate of Arts (A.A.), Associate of Science (A.S.), Associate of Science in Teaching (A.S.T.), and Associate of Fine Arts (A.F.A.).

1. Communication: 9 semester hours

a. Six (6) semester hours of English composition and three (3) semester hours in English oral presentational communication are required.

2. Humanities and/or Fine Arts: 9 semester hours

a. One course must be in literature.

3. Social/Behavioral Sciences: 6 semester hours

4. History: 6 semester hours

5. Natural Sciences: 8 semester hours

6. Mathematics: 3 semester hours

C. Courses specified as meeting general education requirements are published in the catalog of each institution.

D. Students pursuing an Associate of Fine Arts degree in Music as a Tennessee Transfer Pathway will complete all of the required general education hours in Section B. above except for six hours of the humanities requirement, including one course in literature, which must be completed at a university upon transfer.

II. Degree Requirements and Provisions

A. All Associate of Arts and Associate of Science degrees offered by institutions in the Tennessee Board of Regents System shall be designated on the THEC Academic Program inventory as University Parallel degrees and require a maximum of 60 semester hours except in certain degree programs in which approval to exceed the maximum has been granted. The programs approved as exceptions to the maximum are identified in institutional catalogs. For students who complete a Tennessee Transfer Pathway, the corresponding Associate of Arts, Associate of Science, or Associate of Fine Arts degree shall include the title of the pathway in the catalog and on the diploma.

B. Students pursuing an Associate of Arts degree shall be required to demonstrate proficiency in a foreign language equivalent to completing of one year of college-level work.

C. The Associate of Applied Science (A.A.S.) degree is not generally designed to transfer to baccalaureate programs without the creation of specific articulation agreements; however, a general education component is required.

D. The following distribution of general education core courses is required for the A.A.S. degree in all community colleges within the Tennessee Board of Regents System:

1. English Composition: 3 semester hours

2. *Humanities and/or Fine Arts: 3 semester hours

3. *Social/Behavioral Sciences: 3 semester hours

4. *Natural Science/Mathematics: 3-4 semester hours

5. One additional course from the categories of Communication, Humanities and/or Fine Arts, Social/Behavioral Sciences, or Natural Science/Mathematics 3-4 semester hours

E. Total 15-17 semester hours

F. *Specific courses satisfying these requirements must be the same courses that satisfy the general education core requirement for the Associate of Arts or Associate of Science degrees.

III. Core Course Approval

A. Each community college will list its general education core courses in its catalog and on its website where appropriate.
B. All core courses must be approved by the systemwide Core Review Committee.
C. The Core Review Committee will include one representative from each community college as appointed by its Chief Academic Officer.
D. The Core Review Committee may include one representative from each of the six locally governed TN public universities and one from the UT system.

IV. Transfer Provisions of the General Education Core and

A. Community college students who do not complete the Associate of Arts, Associate of Science, Associate of Science in Teaching, or Associate of Fine Arts degree and transfer to another community college within the Tennessee Board of Regents System but who complete blocks of subject categories will have satisfied the general education requirements for the categories of note.

1. For example, if the eight (8) semester hours of natural sciences are completed, then this block of the general education requirement is fulfilled upon transfer to another community college within the Tennessee Board of Regents System.

2. When a subject category is incomplete, a course by-course evaluation will be conducted, and the student will be subject to specific requirements of the receiving institution

Sources

Authority

T.C.A. § 49-8-203; THEC; SACS

Exhibit

2025 TBR Core Model

History

TBR Meetings, June 25, 1976; June 25, 1982; March 20, 1987; June 24, 1988; December 5, 1997; June 29, 2004; September 24, 2004; March 27, 2008; TBR Board Meeting September 25, 2009. TBR Board Meeting, December 2, 2010; September 21, 2012; December 21, 2014 (Removed language in Section I.D. referring to finding the course information on the TBR and/or Policies & Guideline website. This information will now be on the individual institution's website.); (Added a new link for pathways information.) TBR Meeting March 30, 2016; Revised at Board Meeting June 20, 2019.

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT:	Policy 4.02.01.00, Approvals of Agreements and Contracts (formerly 1.03.02.10) (Revisions)
PRESENTER:	Heather Stewart
ACTION REQUIRED:	Requires Vote

Summary:

The substantive proposed revisions to this policy, which have been approved by BASC, are explained below.

(1) The proposed revisions consistently use the term "contract" when referring to any type of document that meets the policy's definition of a contract and that must be reviewed and approved in accordance with policy.

(2) The revisions in Section II.A.9 are to bring the policy into conformance with predominant practices. The documents indicated in the stricken language currently are not routinely submitted for approval by the Chancellor and do not need to be approved by the Chancellor (unless required by a separate provision of the policy).

(3) Section II.A.10 is designed primarily to ensure that the Chancellor approves any contract in which student information will be shared with a researcher pursuant to FERPA's "studies" exception. This provision applies only to the sharing of student information pursuant to the FERPA provisions identified in the policy, and does not include sharing of student information authorized by other FERPA provisions, specifically including, but not limited to, outsourcing of services that could be performed by school officials.

(4) Section II.A.11 clarifies that TCAT contracts must be approved by the Chancellor, unless there is a specific exception.

Attachment

4.02.01.00 Approvals of Agreements and Contracts (formerly 1:03:02:10)

Policy/Guideline Area

Business and Finance Policies

Applicable Divisions

TCATs, Community Colleges, System Office

Purpose

The following policy ~~on approvals is adopted by the Tennessee Board of Regents (TBR) to~~ identifies which ~~delineate the approval process for~~ procurements and ~~agreements~~ contracts must be approved by the TBR System Office. ~~to be entered into by institutions governed by the TBR.~~

Definitions

- Contract – An agreement between parties which obliges each party to take or not take certain actions. Contracts may be called any number of things, including, but ~~are~~ not limited to, agreement, memorandum of understanding, memorandum of agreement, purchase order, procurement, letter of intent, and terms and conditions.
- Institution – means any of the community colleges, colleges of applied technology and System Office departments within the Tennessee Board of Regents (TBR) system.
- System Office – the administrative offices of the Tennessee Board of Regents.

Policy/Guideline

I. Approval By Presidents

A. All agreements and contracts affecting an institution must be approved and executed by the President or the President's designee.

B. Each institution may ~~shall~~ develop written policies and procedures ~~which are~~ in addition to TBR~~'s~~ policies and guidelines, as necessary, to ~~and which will~~ further ensure that no contract or agreement is entered into without the approval of the President or the President's designee, and where necessary, by the Chancellor.

II. Approval By Chancellor

A. The following ~~agreements,~~ contracts, ~~in~~including ~~or~~ procurements, in addition to being approved as set out above, shall be submitted to the System Office Procurement, Contracts, and Payment Services Department for approval by the Chancellor or the Chancellor's designee:

1. ~~Agreements and C~~contracts involving or related to the purchase or disposal of real property, insurance, and capital outlay projects.

2. ~~Agreements~~ Contracts involving or related to the leasing (institution as lessee or lessor) of real property for more than five (5) years or more than $150,000 per year.

3. Any contract ~~agreement~~, including a purchase order~~s~~, for two hundred fifty thousand dollars ($250,000) or more in annual revenue or expense.

~~3.~~4. Any noncompetitive contract with a potential term of more than one (1) year and a cumulative value of two hundred fifty thousand dollars ($250,000) or more. Institutions shall not enter into multiple one-year contracts, involving the same vendor for the same service, to circumvent this requirement~~.~~

~~4.~~5. ~~Agreements and C~~contracts involving insurance or other benefits.

~~5.~~6. Contracts~~Agreements~~ in which the TBR is a named party.

~~6.~~7. The primary operating contract ~~agreement~~ between an institution and its foundation and any other contract ~~agreement~~ between the institution and its foundation which does not conform to the requirements of G-030, Contracts Guideline.~~TBR Guideline G-030 (Contracts Guideline).~~

~~7.~~8. Contracts, including grant agreements, which do not conform to the requirements of G-030, Contracts Guideline.~~TBR Guideline G-030~~

~~8.~~9. Banking, procurement card and other financial services contracts ~~agreements~~.

~~a. Any agreement between a TBR institution and any other institution, agency, organization or entity which provides for the coordinated or cooperative offering of any credit or non-credit programs or activities or in which certificate or degree requirements are met or credit is given for coursework or activities offered by another institution.~~

~~b. Examples of such agreements include provisions for either credit or non-credit academic programs or public service activities to private or state agencies and institutions in the fulfillment of that agency' s responsibility for state-wide services or governmental training, and~~

~~Agreements which require consortia or cooperative arrangements with other institutions, agencies, or associations.~~

10. ~~Any noncompetitive contract with a potential term of more than one (1) year and a cumulative value of two hundred fifty thousand dollars ($250,000) or more. Institutions shall not enter into multiple one-year contracts, involving the same vendor for the same service, to circumvent this requirement.~~Any contract with an organization conducting a study (as permitted by 34 C.F.R. § 99.31(a)(6), to develop, validate or administer predictive tests; to administer student aid programs; or to improve instruction) that may obligate a college to share information relating to a student. *I.e.*, the "studies exception" in FERPA that permits colleges to share personally identifiable student information under limited circumstances.

~~9.~~11. Any contract executed on behalf of a TCAT or in which a TCAT is a party, unless there is a policy provision exempting the contract from review.

B. Renewals of the above contracts~~agreements~~ do not require approval by the Chancellor or the Chancellor's designee if no changes have been made. However, a copy of the executed renewal shall be provided to the System Office.

~~B.~~C. Contracts between a TBR institution and another entity providing for the coordinated offering of a credit program are not required to be submitted to the System Office for approval, unless required by another TBR policy. E.g., 2.01.00.05 Early Postsecondary Opportunities.

~~C.~~D. Purchase orders issued pursuant to purchase orders and/or contracts which have already been approved by the Chancellor or the Chancellor's designee do not require additional approval by ~~to~~ the System Office.

~~D.~~E. The Chancellor may direct that certain or all contracts ~~agreements~~ of any i~~I~~nstitution be submitted for prior System Office review and approval.

III. Other Approvals

A. Certain contracts ~~agreements~~ may be subject to additional review and/or approval processes as set out in TBR policies, i.e. Fiscal Review, State Building Commission, etc.

IV. Exceptions

A. The Chancellor or designee may approve exceptions to the requirements of this policy in appropriate circumstances. Requests for exceptions must be signed by the President and include sufficient justification documentation.

Sources

Authority

T.C.A. § 49-8-203; All State and Federal statutes, codes, and/or rules referenced in this policy and Guideline G-030- Contracts Guideline.

History

TBR Meetings, March 5, 1976; June 26, 1981; September 30, 1983; December 13, 1985; September 22, 1989; June 28, 1991; December 5, 1997; December 2, 2005.

Revision approved by Board, September 15, 2016; Ministerial change to B & F policy June 25, 2019.

Related Polices

4.02.10.00 Purchasing Policy

G-030 Contracts Guideline

4.02.20.00 Disposal of Surplus Personal Property

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT:	Guideline G-035 Non-Credit Programs (New Guideline) Policy 9.01.03.00, Advertising (Revisions)
PRESENTER:	Heather Stewart
ACTION REQUIRED:	Requires Vote

Summary:

To help ensure that *non-credit* programs provide appropriate value and are marketed in accordance with applicable marketing policies and requirements, G-035 is being proposed as a new guideline. Revisions to 9.01.03.00, which are consistent with G-035, are also being proposed. G-035 does not apply to classes offered for credit.

The goal of G-035 is to ensure that the President of each College has developed a process (individualized and suitable to the College) to review non-credit programs and to make sure they provide sufficient quality and appropriate value. Non-credit programs offered by third parties, or which are offered in partnership with third parties, likely need closer scrutiny than those developed and offered by faculty within the TBR system. For example, certain IT bootcamps created and taught by third parties may cost much more than Community College tuition. Such programs must be evaluated for quality and value. Contracts for such programs (regardless of what the document is called) must be reviewed in accordance with the requirements for reviewing all contracts, including that the President approve the contract.

G-035, as well as the revisions to 9.01.03.00, are intended to make clear that non-credit programs must be marketed in accordance with relevant marketing policies, including that such marketing is subject to review and approval by the College's Chief Marketing Officer.

G-035 does not implement any new requirements for the College to notify the System Office about non-credit programs, but rather formalizes the existing requirement.

G-035 and 9.01.03.00 have been reviewed by the Chief Marketing Officers and Workforce Development Officers. BASC reviewed and approved G-035.

Attachments

G-035 Non-Credit Programs

Policy/Guideline Area

General Guidelines

Applicable Divisions

TCATs, Community Colleges

Purpose

This guideline is designed to ensure the provision of appropriate non-credit program offerings and to give the System Office notice of non-credit programs. This guideline does not apply to for-credit programs.

Policy/Guideline

I. Standards

A. Non-credit programs must reflect the TBR System's standards and reputation for providing quality educational programs and delivering value.

B. Non-credit programs must be marketed in accordance with TBR's Marketing and Communications policies, including, but not limited to TBR Policy 9.01.03.00, Advertising, and are subject to review and approval by the college's Chief Marketing Officer.

C. Any arrangement or agreement, regardless of the name of the document, with an entity or person other than the college to provide a non-credit program through a college is a contract and must comply with applicable policies and guidelines regarding contracts and contract approval, including the requirement that the President approve the contract.

D. When a college enters into a contract to offer a non-credit course, special care must be taken to ensure compliance with TBR standards, policies, and requirements.

E. Each President is responsible for implementing a review and approval process to ensure that non-credit programs meet the college's quality standards and provide sufficient value. The President has discretion to create a review and approval process appropriate for the college.

F. Colleges must exercise due care to make sure that third parties do not inappropriately use the institution's name, reputation, or trademarks.

II. System Office Notice Requirements

A. Each college must notify the System Office of all non-credit program offerings in accordance with processes available on the Center for Workforce Development website. See https://www.tbr.edu/cwd/non-credit-instruction-industry-training-reporting

Sources

Authority

T.C.A. § 49-8-203

History

New Guideline August _, 2024.

Related Polices

9.01.03.00 Advertising (formerly 4.06.00.00)

Policy/Guideline Area

Marketing and Communications

Applicable Divisions

TCATs, Community Colleges, System Office

Purpose

This policy governs the procurement of external media advertising by the College. To maintain brand integrity and consistency, all advertisements must incorporate established graphic identity, embody key strategic messages, and strictly adhere to comprehensive guidelines and standards. Advertising should enhance the College's visibility while ensuring a unified and professional representation of the College in all advertising endeavors.

Definitions

Advertising - Advertising refers to the paid or unpaid placement of messages promoting the College in various media platforms. This includes, but is not limited to, print or electronic publications, websites, radio, television, social media platforms, video, or other means of electronic distribution (such as podcasts); and on public media such as banners, billboards, kiosks, and other signage.

Definitions included in the overarching Marketing and Communications Policy (9.01.00.00) apply.

Policy/Guideline

I. Placement

A. Purchasing of advertising is permitted in external media to enhance the perception of the College among its various constituencies; to provide accurate and timely information about College programs, events, and services; to provide legal notice where required by law; and to inform the public of employment opportunities; and for other purposes consistent with the College's mission.

1. Advertising for the recruitment of students shall be designed to increase enrollments in the service delivery area as the first priority for advertising.
2. Any advertising for Colleges in regional publications shall be restricted to zoned editions.
3. Any advertising for Colleges should be within their assigned service areas.
4. Advertising expenditures should result in a citizenry which is better informed and thus more likely to support state higher education through both private giving and more effective advocacy.

5. Advertising also informs citizens of the opportunities available through the state's higher education institutions, thus improving the state's workforce and competitive position in the global economy.
6. Colleges are encouraged to maintain an appreciation of the efforts of all post-secondary institutions to provide educational services to students. In this sense, advertising for one college should not be designed in a manner that has the impact of being detrimental with regard to the educational services provided by another college.

B. The Chief Marketing Officer (CMO) must oversee and approve the content, placement, and purchase of all College advertising. The CMO maintains the authority to remove any advertising from distribution.

1. Colleges should document appropriate procedures for units, programs, and initiatives in local policy or guidelines to request advertising placement.

C. All advertising must be designed to meet professional quality standards in design and content as determined by the CMO.

D. All advertising must be purchased in compliance with all applicable local, state, and federal laws, and TBR and College policies, guidelines, and procedures.

E. Colleges must use System-wide contracts for advertising if available. Exception requests can be submitted to the System Chief Marketing Officer (SCMO), who will consult with the Office of Business and Finance and the Office of General Counsel.

F. All advertising must align with the pre-established marketing, branding, and communications guidelines and applicable policies to ensure key messages are disseminated in a manner that maintains consistency.

II. Reporting

A. CMOs shall evaluate paid advertising annually to determine if the return on investment justifies continued use of the advertising. A "cost to benefit" analysis of paid advertising should be a significant factor in the determination of whether or not to continue the advertising campaign, along with other factors deemed appropriate by the President.

B. A report should be given to the SCMO on previous fiscal year advertising expenditures by August 1 each year.

III. Truthfulness and Substantiation

A. All advertising must follow local, state, and federal laws regarding truth in advertising and other consumer protection laws.

B. The Federal Trade Commission Act and the Isakson and Roe Act dictate that advertising must be truthful, not misleading, and, when appropriate, backed by scientific evidence, regardless of the placement of the advertisement.

C. All advertising must follow the TBR Policy 9.01.02.00, Publications) in reporting advertising materials as publications.

IV. Privacy and Data Collection

A. All advertising should follow applicable local, state, and federal data privacy laws, as well as applicable privacy policies, specifically including, but not limited to those relating to student education records and personally identifiable information.

V. Advertising on College Websites and Publications

A. Use of College resources to promote or advertise activities or entities unrelated to the College is prohibited unless such use is consistent with the mission of the College and results in substantial benefit to the College as determined by the CMO.

B. The sale of advertising in student publications, auxiliary operations, and athletics-related programs are expressly permitted.

VI. Advertising of Non-Credit Programs

A. Advertising of non-credit programs is subject to TBR and College marketing policies.

B. When a College advertises or offers a non-credit course or program that will not result in a credential issued by the College, the website, brochure, or other description of the course or program material must make clear that the course will not result in a credential awarded by the College. E.g., "This [BOOTCAMP/CLASS/PROGRAM/COURE OF STUDY] is delivered and promoted by [PROVIDER] in partnership with [NAME OF COLLEGE]. Any credential upon completion will be awarded by [PROVIDER], and not [NAME OF COLLEGE.]"

~~VI.~~VII. Exemptions and Exceptions

A. Exemptions and exceptions outlined in the overarching Marketing and Communications Policy (9.01.00.00) apply.

Sources

Authority

T.C.A. § 49-8-203

History

TBR Meeting December 4, 1998; September 28, 2007; September 12, 2023, Board approved (formerly 4.06.00.00).

Related Polices

9.01.02.00 Publications (formerly G-140)

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT:	Proposed New Guideline A-115, Foreign Talent Recruitment Programs
PRESENTER:	Heather Stewart
ACTION REQUIRED:	Requires Vote

Summary:

Proposed Guideline A-115, Foreign Talent Recruitment Programs, is designed to comply with the CHIPS and Science Act (the Act), which requires that institutions of higher education implement a policy/guideline by August 7, 2024. Unfortunately, TBR only recently learned about this requirement, which has not received significant publicity.

The Act and Guideline A-115 require two basic actions. First, individuals significantly involved in conducting federally funded research activities (generally the PI and any co-PIs) must disclose participation in a "Foreign Talent Recruitment Program" (FTRP). FTRP has a lengthy definition, but essentially means a program run by a foreign country or entity that offers faculty and other employees money and non-monetary compensation for their services. Second, such individuals are prohibited from participating in a Malign Foreign Talent Recruitment Program, which, generally speaking, is a FTRP run for a prohibited purpose by China, North, Korea, Russia, Iran, or an entity based in such a country.

The Act and Guideline require that covered individuals disclose to the College whether they are participating in a FTRP annually and upon applying for a federal grant. The College has discretion to determine how such disclosures are made, such as to the IRB or through the conflict of interest reporting system. At least one administrator is responsible for reviewing disclosures to ensure compliance with the Act.

The Act and Guideline contain a list of permissible international collaboration activities.

The TBR System Office is in the process of evaluating how to comply with Tennessee Public Chapter 955, which requires implementation of a research security policy by January 1, 2024. (This topic was discussed with the Academic Affairs and Faculty

Subcouncils in July, but no draft revisions were shared because the TBR Staff is still evaluating federal guidance issued July 23, 2024.) Most likely, TBR Staff will recommend revision of Policy 2.08.00.00, General Policies Regarding Research, to comply with PC 955. It is very possible that TBR staff will recommend incorporating Guideline A-115 into 2.08.00.00.

Attachment

A-115 Foreign Talent Recruitment Programs

Policy/Guideline Area

Academic Guidelines

Applicable Divisions

TCATs, Community Colleges, System Office

Purpose

To comply with federal law and to require that all Covered Individuals (1) disclose any participation in a Foreign Talent Recruitment Program and (2) certify that they are not participating in a Malign Foreign Talent Recruitment Program.

Policy/Guideline

I. Disclosure by Covered Individuals

A. Any College or System Office faculty or staff member defined as a Covered Individual who is engaged in U.S. federally funded research activities must disclose participation in a Foreign Talent Recruitment Program. If participating in a Foreign Talent Recruitment Program, a Covered Individual must certify that they are not participating in a Malign Foreign Talent Recruitment Program.

B. For federal grant applications, investigators and senior/key personnel will be required to disclose any Foreign Talent Recruitment Program participation at the time of grant submission. The principal investigator, as well as any co-principal investigators and others identified by the principal investigator, are also required to certify that they do not participate in any Malign Foreign Talent Recruitment Program.

C. Disclosures must be made to the College, both annually and upon submission of any federal grant application, in a manner directed by the College (e.g., through the College's Conflict of Interest disclosure system or through the College's Institutional Review Board).

D. The College shall appoint one or more administrators responsible for:

1. Reviewing disclosures by Covered Individuals and verifying the accuracy and completeness of the information provided, and assessing whether participation in the Foreign Talent Recruitment Program aligns with TBR and college policies and complies with federal regulations;

2. Providing guidance to Covered Individuals on compliance with this policy;

3. If potential involvement with a Malign Foreign Talent Recruitment Program is identified, undertaking further investigation, and taking appropriate action, which may include obtaining legal advice from the Office of General Counsel, recommending suspension of certain activities, and taking corrective measures;

4. Maintaining accurate records of all disclosures and taking action to ensure ongoing compliance with this policy, including reviews of research activities as necessary; and

5. Providing training to faculty and staff about disclosure requirements, the implications of participation in a Foreign Talent Recruitment Program, and the implications of non-compliance.

E. Covered Individuals are prohibited from participating in a Malign Foreign Talent Recruitment Program, in accordance with the CHIPS and Science Act of 2022 and National Security Presidential Memorandum-33.

II. DEFINITIONS

A. “Covered Individual” means any College or System Office faculty or staff member who is funded by a federal award and contributes in a substantive, meaningful way to the scientific development or execution of a research and development project proposed to be carried out with a research and development award from a federal research agency and is designated as a covered individual by the federal research agency concerned. Colleges shall consider the principal investigator, as well as any co-principal investigators to be Covered Individuals and require that they provide applicable disclosures and certifications.

B. “Foreign Talent Recruitment Program” means any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether or not directly or indirectly stated in the arrangement, contract, or other documentation at issue.

C. “Malign Foreign Talent Recruitment Program” means any Foreign Talent Recruitment Program that meets both Subsection II.C.1. and II.C.2.

1. Where compensation or remuneration from any foreign country is provided to the Covered Individual in exchange for any of the following:

    a. Engaging in the unauthorized transfer of intellectual property, materials, data products, or other nonpublic information owned by a U.S. entity or developed with a U.S. federal research and development award to the government of a foreign country or an entity based in, funded by, or affiliated with a foreign country regardless of whether that government or entity provided support for the development of the intellectual property, materials, or data products;

    b. Being required by a foreign country to recruit trainees or researchers to enroll in such program, position, or activity;

    c. Establishing a laboratory or company, accepting a faculty position, or undertaking any other employment or appointment in a foreign country or with an entity based in, funded by, or affiliated with a foreign country if such activities are in violation of the standard terms and conditions of a U.S. federal research and development award;

    d. Being unable to terminate the Foreign Talent Recruitment Program contract or agreement except in extraordinary circumstances;

    e. Through funding or effort related to the Foreign Talent Recruitment Program, being limited in the capacity to carry out a research and development award or required to engage in work that would result in substantial overlap or duplication with a federal research and development award;

    f. Being required to apply for and successfully receive funding from the sponsoring foreign government's funding agencies with the sponsoring foreign organization as the recipient;

    g. Being required to omit acknowledgment of the recipient institution with which the individual is affiliated, or the U.S. federal research agency sponsoring the research and development award, contrary to the institutional policies or standard terms and conditions of the U.S. federal research and development award;

    h. Being required to not disclose to the U.S. federal research agency or employing organization the participation of a Covered Individual in such program, position, or activity; or

i. Having a conflict of interest or conflict of commitment contrary to the standard terms and conditions of the U.S. federal research and development award.

2. Where a Covered Individual is sponsored or supported either:

a. by a foreign country of concern (currently China, North Korea, Russia, or Iran) or an entity based in a foreign country of concern (whether or not directly sponsored by the foreign country of concern); or

b. An academic institution or foreign talent recruitment program on the list developed under §1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 4001 note; Public Law 115–232) available at https://basicresearch.defense.gov.

D. Acceptable International Collaboration Activities. A Foreign Talent Recruitment Program does not include the following international collaboration activities, so long as the activity is not funded, organized, or managed by an academic institution or a Foreign Talent Recruitment Program identified in Section II.C.2.

1. Making scholarly presentations and publishing written materials regarding scientific information not otherwise controlled under current law;

2. Participating in international conferences or other international exchanges, research projects, or programs that involve open and reciprocal exchange of scientific information, and which are aimed at advancing international scientific understanding and not otherwise controlled under current law;

3. Advising a foreign student enrolled at an institution of higher education or writing a recommendation for such a student, at such student's request;

4. Engaging in the following international activities:

a. Activities that are partly sponsored or otherwise supported by the United States such as serving as a government appointee to the board of a joint scientific fund (e.g., the U.S. – Israel Binational Industrial Research and Development Foundation); providing advice to or otherwise participating in international technical organizations, multilateral scientific organizations, and standards setting bodies (e.g., the International Telecommunications Union, Intergovernmental Panel on Climate Change, etc.); participating in a Fulbright Commission program funded in whole or in part by a host country government; or other routine international scientific exchanges and interactions such as providing invited lectures or participating in international peer review panels.

b. Involvement in national or international academies or professional societies that produce publications in the open scientific literature that are not in conflict with the interests of the federal research agency (e.g., membership in the Pontifical Academy of Sciences or The Royal Society).

c. Taking a sabbatical, serving as a visiting scholar, or engaging in continuing education activities such as receiving a doctorate or professional certification at an institution of higher education (e.g., the University of Oxford, McGill University) that are not in conflict with the interests of the U.S. federal research agency.

d. Receiving awards for research and development which serve to enhance the prestige of the U.S. federal research agency (e.g., the Nobel Prize).

e. Other international activities determined appropriate by the U.S. federal research agency head or designee.

Sources

Authority

T.C.A. § 49-8-203;

History

New Guideline August _, 2024.

References

OSTP Foreign Talent Recruitment Program Guidelines. (2024). https://www.whitehouse.gov/wp-content/uploads/2024/02/OSTP-Foreign-Talent-Recruitment-Program-Guidelines.pdf.

CHIPS & Science Act of 2022, 42 U.S.C. §19232; Public Law 116-167 (2022). https://uscodeweb1.house.gov/view.xhtml?path=/prelim@title42/chapter163/subchapter6/partC&edition=prelim.

NSPM-33 United States Government-Supported Research and Development National Security Policy (2021). https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/
Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, 10 U.S.C. 4001 note; Public Law 115–232. https://uscode.house.gov/statviewer.htm?volume=132&page=2078#

Related Polices

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT:	Policy 6.04.00.00, Pregnancy, Childbirth, and Related Medical Conditions (Revisions)
PRESENTER:	Heather Stewart
ACTION REQUIRED:	Requires Vote

Summary:

Proposed revisions to this policy are designed to comply with regulations that implement the Pregnant Workers Fairness Act. (Please note that this policy applies to employees and expands Title VII protections. The revisions are not based on the Title IX regulations, which have been enjoined.) The revisions accomplish the following primary purposes, as required by the regulations:

(1) Clarify that the policy applies to employees.

(2) Require that when an employee informs a supervisor that she is pregnant, the supervisor tell the employee how to request a reasonable accommodation.

(3) Limit the documentation that HR may request and obtain from an employee to that which is reasonable under the circumstances. The College is not permitted to request excessive or unnecessary documentation.

(4) Clarify that unpaid leave can be a form of reasonable accommodation.

The HR Officers and BASC have approved these revisions.

Attachment

6.04.00.00 Pregnancy, Childbirth, and Related Medical Conditions (Employees)

Policy/Guideline Area

Sexual Discrimination/Harassment/Misconduct

Applicable Division

TCATs, Community Colleges, System Office

Purpose

The Tennessee Board of Regents prohibits discrimination against employees because of sex and requires institutions to comply with all legal obligations regarding pregnancy, childbirth, and related medical conditions in accordance with Title VII of the Civil Rights Act of 1964, the Pregnant Workers Fairness Act, Title IX of the Education Amendments of 1972, the PUMP Act, Tennessee Code Annotated § 50-1-305, and all other applicable state and federal statutes and regulations.

Definitions

- "Institution" means each college within the TBR System~~,~~ and includes the TBR System Office.
- "Known limitation" means a physical or mental condition related to, affected by, or arising out of pregnancy, childbirth or related medical conditions that the employee or the employee's representative has communicated to the institution, whether or not such condition constitutes a disability under the Americans with Disabilities Act.
- "~~Qualified E~~employee" means an employee or applicant who, either with or without reasonable accommodation, can perform the essential functions of the job position. An employee or applicant is considered qualified if any inability to perform an essential function is for a temporary period, the essential function can be performed in the near future, and the inability to perform the essential function can be reasonably accommodated.
    - This policy applies to all qualified employees of the institution, whether full- or part-time; whether faculty, adjunct, or staff; P-080, Discrimination & Harassment -- Complaint Investigation Procedure and regardless of length of employment.

- A qualified applicant is considered to be a qualified employee.

- "Reasonable accommodation" generally has the same meaning as under the ADA.
  - Reasonable accommodation means a modification or adjustment to a job or the work environment that will enable a qualified employee to perform the essential functions of the job. (Unlike the ADA, reasonable accommodation under this policy may include temporarily relieving a qualified employee of an essential function of the job.) If multiple reasonable accommodations are available, the institution may select among reasonable accommodations.
  - Reasonable accommodation may include, but is not limited to, making existing facilities accessible, leave, job restructuring, a part-time or modified work schedule, acquiring or modifying equipment, changing or making exceptions to a policy, and reassignment to a vacant position.

- "Related medical condition" includes any illness, complication, or symptoms arising out of pregnancy or childbirth. Examples of related medical conditions include, but are not limited to, morning sickness, gestational diabetes, pregnancy-induced hypertension, miscarriage, sciatica, lactation or the need to express breast milk, medical procedures and recovery, physical injuries from childbirth, and postpartum depression.

Policy/Guideline

I. Nondiscrimination in General

A. Discrimination or harassment based on current, potential, or past pregnancy, or related medical condition, is prohibited ~~gender~~ sex discrimination. Complaints of discrimination or harassment based on any alleged violation of this policy~~pregnancy~~ should be submitted to the Title IX Coordinator and will be investigated pursuant to TBR Guideline P-080 Discrimination & Harassment - Complaint Investigation Procedure or TBR Policy 6.01.00.00 Sex Discrimination, Sexual Harassment or Sexual Misconduct.

B. Retaliation against someone who requests a reasonable accommodation for pregnancy, childbirth, or a related medical condition or who files a complaint based on pregnancy is prohibited. Retaliation complaints will be investigated under TBR Guideline P-080 Discrimination & Harassment - Complaint Investigation Procedure or TBR Policy 6.01.00.00 Sex Discrimination, Sexual Harassment or Sexual Misconduct.

C. An institution shall treat employees who are temporarily unable to perform their job duties or participate in educational programs due to pregnancy, childbirth, or related medical conditions the same as non-pregnant employees who are similar in their ability or inability to work or participate in educational activities, for example with respect to temporary and light duty assignments.

II. Reasonable Accommodation on the Basis of Pregnancy, Childbirth, and Related Medical Conditions

A. Anyone ~~employee or applicant who~~ seeking~~s~~ a reasonable accommodation under this policy should contact the institution's Title IX Coordinator or other individual designated by the institution. Employees are required to participate in an interactive process to determine a reasonable accommodation. A request for accommodation may be made orally or in writing.

B. ~~An employee who learns that another employee may need reasonable accommodation under this policy should~~ must report the matter to the Title IX Coordinator or other individual designated by the institution. Anyone with regular supervisory responsibilities over an employee who learns from the employee or employee's representative about a potential need for a reasonable accommodation due to pregnancy, childbirth, or a related medical condition must inform the employee or representative how to request a reasonable accommodation and must inform the Title IX Coordinator or other person designated by the institution about the employee's need for a potential accommodation. ~~supervisor, manager, anyone who regularly directs the~~

~~employee, any human resources personnel or other appropriate official who learns from a qualified employee or from the qualified employee's representative of a known limitation and a need for an accommodation must inform the employee of how to make a request for a reasonable accommodation and the person to whom the request should be made and must also contact the Title IX Coordinator to ensure that the reasonable accommodation is made or the interactive process begun.~~

C. An institution shall make reasonable accommodation to known limitations related to pregnancy, childbirth, or related medical condition of a qualified employee. The institution and employee must engage in a good faith, interactive process to identify a reasonable accommodation.

D. An institution may deny a reasonable accommodation if it would result in undue hardship to the institution. The Office of General Counsel must be consulted prior to denying a reasonable accommodation based on undue hardship.

~~D.~~E. Any request for documentation for pregnancy, childbirth, or a related medical condition must be made by the human resources department. The human resources department may only ask for documentation that is reasonable under the circumstances to determine a reasonable accommodation, and any request must comply with the limitations on requests for information in TBR Policy 5.01.01.14 Family, Medical, and Service Member Leave. ~~An institution may not seek unreasonable supporting documentation. An institution may only request medical documentation if necessary. Any necessary and reasonable requests for supporting documentation are limited to confirming the medical condition, confirming that the condition is related to, affected by or arising out of pregnancy, childbirth or related medical condition, and describes the adjustment or change that is needed due to the limitation.~~

~~E.~~F. An institution shall not:

1. require a qualified employee to accept a reasonable accommodation other than one arrived at through an interactive process;
2. deny equal employment opportunities to a qualified employee based on the need to make reasonable accommodations; or
3. take adverse action against a qualified employee because the employee requested or used a reasonable accommodation, or otherwise retaliate against an individual in violation of applicable law.

G. A qualified employee may elect to take leave in accordance with TBR Policy 5.01.01.08, Parental Leave or TBR Policy 5.01.01.14, Family, Medical, and Service Member Leave. An institution shall not require a qualified employee to take leave, whether paid or unpaid, if another reasonable accommodation can be provided. Human Resources is responsible for coordinating leave under various policies.

~~F.~~H. If an employee who is pregnant, gives birth, or has a related medical condition does not have enough leave or does not qualify for leave, the institution must allow the employee to take unpaid leave for a reasonable period of time for pregnancy, childbirth, or a related medical condition, after which the employee must be reinstated to the status held when the leave began or to a comparable position without decrease in pay, loss of promotional opportunity, or other right or privilege of employment.

~~G.~~I. Reasonable accommodation, including unpaid leave, pursuant to this policy is available only to qualified employees who are pregnant, have given birth, or have a pregnancy-related condition. Leave for family members may be available pursuant to TBR Policy 5.01.01.08, Parental Leave or TBR Policy 5.01.01.14, Family, Medical, and Service Member Leave.

III. Lactation

A. An institution shall provide space other than a restroom to express milk. The institution may either create dedicated space or provide temporary space on an as-needed basis. The space must be clean, shielded from view, and free from intrusion from others.

B. Institutions must provide a reasonable amount of break time, as frequently as needed by the nursing mother, to express milk. Breaks must be provided for one year following birth, and any employee who wishes to continue expressing breast milk beyond one year should contact the Title IX Coordinator to discuss additional time to provide breaks.

C. Employees taking breaks to express milk shall be compensated in the same manner as other employees are compensated during break time. No deduction may be made from an exempt employee's salary. No deduction from a non-exempt employee's pay is permitted unless the Title IX Coordinator has approved in advance.

Sources

Tenn. Code Ann. § 50-1-305

Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e et seq. (as amended by the Pregnant Workers Fairness Act); 29 C.F.R. Part 1636

Title IX of the Education Amendments of 1972, 20 U.S.C. §§ 1681-1688

Fair Labor Standards Act § 18d (as amended by the Providing Urgent Maternal Protections for Nursing Mothers Act (PUMP Act))

History

TBR Board Meeting, June 16, 2023; TBR Board Meeting _____, 2024.

Related Polices

5.01.01.08 Parental Leave

5.01.01.14 Family, Medical, and Service Member Leave

6.01.00.00 Sex Discrimination, Sexual Harassment or Sexual Misconduct

6.02.00.00 Sex Discrimination and Sexual Harassment

6.03.00.00 Sexual Misconduct

P-080 Discrimination & Harassment - Complaint & Investigation Procedure

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT: Personally Identifiable Information Policy 1.08.04.00

PRESENTER: Jon Calisi

LENGTH OF PRESENTATION: *(5 minutes)*

ACTION REQUIRED: Requires Vote

Summary:

TBR institutions create, collect, maintain, use, and transmit personally identifiable information relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. TBR institutions are committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations.

The proposed revisions, which have been approved by the IT Sub council, are attached in tracked changes and clean copy form.

Personally Identifiable Information (PII) 1.08.04.00 (formerly G-053)

Policy Area

Governance, Organization, and General Policies

Applicable Divisions

TCATs, Community Colleges, System Office, Board Members

Purpose

TBR institutions create, collect, maintain, use, and transmit personally identifiable information relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. TBR institutions are committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations.

Definitions

- Data Custodians - Data Custodians are the people responsible for oversight of personally-identifiable information in their respective areas of institutional operations.
- The Data Custodian (also called a Data Steward or Data Owner) is the person who has administrative control and has been officially designated as accountable for a specific information asset or dataset. This person would determine who has access to what and IT implements the controls to match.
- Minimum Necessary - Minimum Necessary is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.
- Personally Identifiable Information (PII) - Information that has not been lawfully made publicly available and which can be used to distinguish or trace an individual's identity, such as Social Security number driver license, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Certain privacy laws, and policies based on those laws, may use a different definition of PII.

- Directory information - Directory information is information that is generally not considered harmful or an invasion of privacy if released. It can also be disclosed to outside organizations.

Policy

I. Policy

A. Members of the TBR community shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it.

B. All individuals who dispense, receive, and store PII have responsibilities to safeguard it.

C. In adopting this policy, the System is guided by the following objectives:

1. To enhance individual privacy for members of the TBR community through the secure handling of PII.
2. To ensure that all members of the TBR community understand their obligations and individual responsibilities under this policy by providing appropriate training that shall permit the TBR community to comply with both the letter and the spirit of all applicable privacy legislation. Each member institution will be responsible for determining the means of training for its institution.
3. To increase security and management of Social Security numbers (SSNs) by:
    a. Instilling broad awareness of the confidential nature of the SSNs;
    b. Establishing a consistent policy about the use of SSNs throughout the System; and
    c. Ensuring that access to SSNs for the purpose of conducting TBR business is granted only to the extent necessary to accomplish a given task or purpose.

d. To reduce reliance on the SSN for identification purposes as much as possible.

4. To comply with all Payment Card Industry (PCI) standards.
5. To comply with any other applicable and required standards, regulations and/or laws.
6. To comply with Family Educational Rights and Privacy Act of 1974 (FERPA).

D. Data Custodians are responsible for oversight of personally identifiable information in their respective areas of institutional operations. Activities of these officials are aligned and integrated through appropriate coordination among these cognizant institutional officials.

II. Scope

A. This policy applies to all members of the TBR community, including all full- and part-time employees, faculty, students, and other individuals such as volunteers, contractors, consultants, other agents of the institution or whose work gives them custodial responsibilities for PII.

III. Policy Requirements

A. Data Custodians

1. Officials responsible for each of the following areas shall be considered Data Custodians:
   a. Student Records
   b. Financial Aid Records
   c. Alumni and Donor Records
   d. Employee Records
   e. Purchasing and Contracts
   f. Research Subjects
   g. Public Safety or Campus Police

IV. Personally Identifiable Information

A. PII may be released only on a Minimum Necessary basis and only to those individuals who are authorized to use such information as part of their official TBR duties, subject to the requirements:
    1. That the PII released is narrowly tailored to a specific operational or business requirement;
    2. That the information is kept secure and used only for the specific operational purposes for which authorization was obtained; and
    3. That the PII is not further disclosed or provided to others without proper authorization.

B. PII may be provided to and handled by third parties, including cloud service providers, with the strict requirement that the information be kept secure and used only for a specific purposes set out in the contract authorizing use of the information.

C. Exceptions to this policy may be made only upon specific requests approved by the institutional official responsible for such information as specified in this policy and only to the degree necessary to achieve the mission and operational needs of the institution.
    1. Exceptions must be documented, retained securely, and reviewed periodically by the appropriate institutional official or his/her designee.
    2. Exceptions may be modified or eliminated based on this review and shall be documented and retained for auditing purposes.

D. Directory Information, as defined by Federal and State law and institutional policy, will be published following the guidelines defined by the specific law.

E. Colleges may share information covered by FERPA only as permitted by FERPA and applicable policy.Colleges must notify students annually of their rights under FERPA.

F. Information that has been collected that conforms to the HIPAA standards of de-identification or anonymization is not PII.

V. Government-Issued Personal Identifiers

A. Social Security Number

1. Provision of Information
    a. TBR institutions collect SSNs:
        1. When required to do so by law;
        2. When no other identifier serves the business purpose; and
        3. When an individual volunteers the SSN as a means of locating or confirming personal records.
    b. In other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.
2. Release of SSNs
    a. SSNs will be released to persons or entities outside the institution only:
        1. As required by law;
        2. When permission is granted by the individual;
        3. When the external entity is acting as the institution's authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties; or
        4. When the Office of General Counsel has approved the release.
3. Use, Display, Storage, Retention, and Disposal
    a. SSNs or any portion thereof will not be used to identify individuals except as required by law or with approval by a TBR official for a TBR operational purpose.
    b. The release or posting of personal information, such as grades or occupational listings, keyed by the SSN or any portion thereof, is prohibited, as is placement of the SSN in files with unrestricted access.

c. SSNs will be transmitted electronically only for operational purposes approved by the institutional officials responsible for SSN oversight and only through secure mechanisms.

d. The Data Custodians who are responsible for SSNs will oversee the establishment of procedures for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.

B. Non-SSN Government-Issued Identifiers

1. In the course of business operations, TBR institutions have access to, collect, and use non-SSN government-issued identifiers such as driver's licenses, passports, HIPAA National Provider Identifiers, Employee Identification Numbers (EIN), and military identification cards, among others.

2. TBR institutions shall follow the Minimum Necessary standard and strive to safeguard these identifiers.

VI. Other Externally-Assigned Identifiers and Other Personally Identifiable Information

A. TBR institutions shall follow the Minimum Necessary standard and strive to safeguard any externally assigned identifiers which may be collected.

VII. Responsibility for Maintenance and Access Control

1. Other institutional offices may maintain and administer electronic and physical repositories containing personal identification numbers for uses in accordance with this policy.

B. Access to electronic and physical repositories containing PII shall be controlled based upon reasonable and appropriate administrative, physical, technical, and organizational safeguards.

C. Individuals who inadvertently gain access to a file or database containing PII should report it to the appropriate authority.

D. All paper documents with PII must be under lock and key or otherwise securely stored.

E. Document retention policies dictate schedules for PII deletion and/or destruction. Proper disposal of PII shall involve cross-cut shredders (for paper), securely wiping/deleting data (for digital information) and other information security approved methods of eliminating this data.

VIII. Enforcement

A. Violations of this policy resulting in misuse of, unauthorized access to, or unauthorized disclosure or distribution of PII may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the institution or, in the case of students, suspension or expulsion from the institution.

Sources

Authority

T.C.A. § 49-8-203

History

NEW Guideline approved at August 19, 2014 President's Meeting; effective September 26, 2014. Revised and changed to policy at Special Called Meeting May 14, 2019.

Personally Identifiable Information (PII) ~~(formerly G-053):~~ 1.08.04.00 (formerly G-053)

Policy Area

Governance, Organization, and General Policies

Applicable Divisions

TCATs, Community Colleges, System Office, Board Members

Purpose

TBR institutions create, collect, maintain, use, and transmit personally identifiable information relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. TBR institutions are committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations ~~in order to maximize trust and integrity~~.

Commented [BL1]: These are not the primary reasons for protecting PII.

Definitions

- Data Custodians - Data Custodians are the people responsible for oversight of personally-identifiable information in their respective areas of institutional operations.
- The Data Custodian ~~Owner~~ (also called a Data Steward or Data Owner) is the person who has administrative control and has been officially designated as accountable for a specific information asset or dataset. This person would determine who has access to what and IT implements the controls to match.
- Minimum Necessary - Minimum Necessary is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.
- Personally Identifiable Information (PII) - Information that has not been lawfully made publicly available and which can be used to distinguish or trace an individual's identity, such as ~~their ID,~~ Social Security number~~,~~ driver license, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Certain privacy laws, and policies based on those laws, may use a different definition of PII.

Commented [BL2]: The policy seems to use Data Custodian the most, so I suggest going with that as the primary term, but I don't have a strong preference, as long as we define the term and use it consistently through policy.

Commented [BL3]: I think that's a pretty good working definition of PII, but I think it would be better to leave open the potential to have a slightly different definition, as there are differences between GLBA, FERPA, and HIPAA.

- Directory information - Directory information is information that is generally not considered harmful or an invasion of privacy if released. It can also be disclosed to outside organizations.

Policy

I. Policy

A. Members of the TBR community shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it.

B. All individuals who dispense, receive, and store PII have responsibilities to safeguard it.

C. In adopting this policy, the System is guided by the following objectives:

1. To enhance individual privacy for members of the TBR community through the secure handling of PII.
2. To ensure that all members of the TBR community understand their obligations and individual responsibilities under this policy by providing appropriate training that shall permit the TBR community to comply with both the letter and the spirit of all applicable privacy legislation. Each member institution will be responsible for determining the means of training for its institution.
3. To increase security and management of Social Security numbers (SSNs) by:
    a. Instilling broad awareness of the confidential nature of the SSNs;
    b. Establishing a consistent policy about the use of SSNs throughout the System; and
    c. Ensuring that access to SSNs for the purpose of conducting TBR business is granted only to the extent necessary to accomplish a given task or purpose.

d. To reduce reliance on the SSN for identification purposes as much as possible.

4. To comply with all Payment Card Industry (PCI) standards.
5. To comply with any other applicable and required standards, regulations and/or laws.
6. To comply with Family Educational Rights and Privacy Act of 1974 (FERPA).

D. Data Custodians are responsible for oversight of personally identifiable information in their respective areas of institutional operations. Activities of these officials are aligned and integrated through appropriate coordination among these cognizant institutional officials.

II. Scope

A. This policy applies to all members of the TBR community, including all full- and part-time employees, faculty, students, ~~and their parents or guardians,~~ and other individuals such as volunteers, contractors, consultants, other agents of the institution ~~community, alumni, and affiliates that are associated with the System~~ or whose work gives them custodial responsibilities for PII.

Commented [BL4]: Alumni and parents aren't bound by policy, unless they are an agent of a college.

III. Policy Requirements

A. Data Custodians~~Trustees~~

1. Officials responsible for each of the following areas shall be considered Dd~~a~~ta Cc~~u~~stodians:
   a. Student Records
   b. Financial Aid Records
   c. Alumni and Donor Records
   d. Employee Records
   e. Purchasing and Contracts
   f. Research Subjects
   g. Public Safety or Campus Police

IV. Personally Identifiable Information

A. PII may be released only on a Minimum Necessary basis and only to those individuals who are authorized to use such information as part of their official TBR duties, subject to the requirements:

1. That the PII released is narrowly tailored to a specific operational or business requirement;
2. That the information is kept secure and used only for the specific operational ~~official TBR [business]~~ purposes for which authorization was obtained; and
3. That the PII is not further disclosed or provided to others without proper authorization ~~as defined above~~.

B. PII may be provided to and handled by third parties, including cloud service providers, with the strict requirement that the information be kept secure and used only for a specific ~~official authorized business~~ purposes set out in the contract authorizing use of the information. ~~as defined in a Business Associate Agreement with that third party.~~

C. Exceptions to this policy may be made only upon specific requests approved by the ~~cognizant~~ institutional official responsible for such information as specified in this policy and only to the degree necessary to achieve the mission and operational~~business~~ needs of the institution.

1. Exceptions ~~made~~ must be documented, retained securely, and reviewed periodically by the appropriate ~~cognizant~~ institutional official or his/her designee.
2. Exceptions may be modified or eliminated based on this review and shall be documented and retained for auditing purposes.

D. Directory Information, as defined by Federal and State law and institutional policy, will be published following the guidelines defined by the specific law.

~~E. Based on FERPA guidelines, directory information is information that is generally not considered harmful or an invasion of privacy if released and can be disclosed~~

Commented [BL5]: Business Associate Agreements are typically used to share PII under HIPAA, which we're not subject to. But the contracts need to set out what information can be used for.

~~without consent.~~ Colleges may share information covered by FERPA only as permitted by FERPA and applicable policy.

~~F.~~E. Colleges~~Schools~~ must notify students annually of their rights under FERPA.

~~G.~~F. Information that has been collected that conforms to the HIPAA standards of de-identification or anonymization is not PII.

V. Government-Issued Personal Identifiers

A. Social Security Number

1. Provision of Information

a. TBR institutions collect SSNs:

1. When required to do so by law;
2. When no other identifier serves the business purpose; and
3. When an individual volunteers the SSN as a means of locating or confirming personal records.

b. In other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.

2. Release of SSNs

a. SSNs will be released to persons or entities outside the institution only:

1. As required by law;
2. When permission is granted by the individual;
3. When the external entity is acting as the institution's authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties; or
4. When the ~~appropriate~~ Office of General Counsel has approved the release.

3. Use, Display, Storage, Retention, and Disposal

Commented [BL6]: This isn't wholly accurate-colleges are required to allow students to opt out of the sharing of directory information. I tried to fix it but think it's better to delete it.

~~c. The Institutional ID is associated permanently and uniquely with the entity to which it is assigned.~~

~~2. Use, Display, Storage, Retention, and Disposal~~

~~a. The Institutional ID is considered PII by the institution, to be used only for appropriate business purposes in support of operations.~~

~~b. The Institutional ID is used to identify, track, and serve individuals across all institutional electronic and paper data systems, applications, and business processes throughout the span of an individual's association with the institution and presence in the institution's systems or records.~~

~~c. The Institutional ID is not to be disclosed or displayed publicly by the Institution, nor to be posted on the institution's electronic information or data systems unless the Institutional ID is protected by access controls that limit access to properly authorized individuals.~~

~~d. The release or posting of personal information keyed by the Institutional ID, such as grades, is prohibited.~~

~~e. Any document, item, file, or database that contains Institutional IDs in print or electronic form is to be protected and disposed of in a secure manner in compliance with data retention rules.~~

~~VII.~~VI. Other Externally-Assigned Identifiers and Other Personally Identifiable Information

A. TBR institutions shall follow the Minimum Necessary standard and strive to safeguard any externally assigned identifiers which may be collected.

~~VIII.~~VII. Responsibility for Maintenance and Access Control

~~A. Institutional IDs are maintained and administered by the appropriate institutional office in accordance with this policy.~~

1. Other institutional offices may maintain and administer electronic and physical repositories containing personal identification numbers for uses in accordance with this policy.

B. Access to electronic and physical repositories containing PII shall be controlled based upon reasonable and appropriate administrative, physical, technical, and organizational safeguards.

C. Individuals who inadvertently gain access to a file or database containing PII should report it to the appropriate authority.

D. All paper documents with PII must be under lock and key or otherwise securely stored.

E. Document retention policies dictate schedules for PII deletion and/or destruction. Proper disposal of PII shall involve cross-cut shredders (for paper), securely wiping/deleting data (for digital information) and other information security approved methods of eliminating this data.

~~IX.~~VIII. Enforcement

A. Violations of this policy resulting in misuse of, unauthorized access to, or unauthorized disclosure or distribution of PII~~personal identification numbers~~ may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the ~~i~~institution or, in the case of students, suspension or expulsion from the institution.

Sources

Authority

T.C.A. § 49-8-203

History

NEW Guideline approved at August 19, 2014 President's Meeting; effective September 26, 2014. Revised and changed to policy at Special Called Meeting May 14, 2019.

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT:	B-090 Safeguarding Nonpublic Financial Information Guideline
PRESENTER:	Jon Calisi
LENGTH OF PRESENTATION:	*(5 minutes)*
ACTION REQUIRED:	Requires Vote

Summary:

This guideline explains the procedure by which Tennessee Board of Regents institutions must develop a comprehensive written Information Security Program (the "Program") as mandated by the Gramm-Leach-Bliley Act ("GLBA") Standards for Safeguarding Customer Information Rule. An institution's Program must include the components described below pursuant to which the institution intends to:

1. Protect the security and confidentiality of customers' nonpublic financial information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

The Program may consist of existing institutional policies and procedures that are incorporated by reference into the Program, including but not limited to policies such as computer/electronic records confidentiality policies, Family Educational Rights & Privacy Act policies, employee/personnel records confidentiality policies, etc..

The proposed revisions, which have been approved by the IT Sub council, are attached in tracked changes and clean copy form.

B-090 Safeguarding Nonpublic Financial Information

Policy/Guideline Area

Business and Finance Guidelines

Applicable Divisions

TCATs, Community Colleges, System Office

Purpose

This guideline explains the procedure by which Tennessee Board of Regents institutions must develop a comprehensive written Information Security Program (the "Program") as mandated by the Gramm-Leach-Bliley Act ("GLBA") Standards for Safeguarding Customer Information Rule. An institution's Program must include the components described below pursuant to which the institution intends to:

1. Protect the security and confidentiality of customers' nonpublic financial information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

The Program may consist of existing institutional policies and procedures that are incorporated by reference into the Program, including but not limited to policies such as computer/electronic records confidentiality policies, Family Educational Rights & Privacy Act policies, employee/personnel records confidentiality policies, etc.

Definitions

- Customer - person who has a continuing relationship with the institution for provision of financial services, such as financial aid.
- Customer Information - any record containing nonpublic personal financial information about a Customer.
- Non-public financial information – any record not publicly available that an institution obtains about a customer in the process of offering a financial product or service, as well as such information provided to the institution by another

source. Nonpublic financial information includes information that a person submits to apply for financial aid (e.g., tax returns and other financial information), that an institution collects from third parties relating to financial aid (e.g., FAFSA information), and that an institution creates based on customer information in its possession.

- Security event – an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

Policy/Guideline

I. Introduction

A. TBR institutions are covered by GLBA because they offer and process financial aid applications, provide loans to students, and receive customer information from students and others in connection with those activities.

B. Each institution must develop, implement, and maintain a written, comprehensive Information Security Program. The Program must contain administrative, technical, and physical safeguards appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. The Program must apply to any paper or electronic record maintained by an institution that contains customer information about an individual or a third party who has a relationship with the institution.

C. Because the TBR System Office handles significant customer information for Tennessee Colleges of Applied Technology through Shared Services, the System Office and the TCATs are considered a single institution for purposes of this policy. Customer information shall be kept confidential and safeguarded by the institution, its affiliates and service providers pursuant to the provisions of the Program and this Guideline.

II. Requirements of an Information Security Program

A. Program Coordinator

1. Except for the TCATs, which will be served by the TBR System Office Program Coordinator, each institution must identify one qualified individual to serve as the Program Coordinator ("Coordinator") who shall be responsible for overseeing and implementing the Program. The Coordinator may obtain assistance from other sources, but ultimate responsibility for the Program remains with the Coordinator.
2. The Coordinator's development of the Program shall include, but not be limited to:
    a. Consulting with the appropriate offices to identify units and areas of the institution with access to customer information and maintaining a list of the same;
    b. Assisting the appropriate offices of the institution in identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and making certain that appropriate safeguards are designed and implemented in each office and throughout the institution to safeguard the protected data
    c. Working with the institution's contract officer(s) to guarantee that all contracts with third party service providers that have access to and maintain customer information include a provision requiring that the service provider maintain appropriate safeguards for customer information; and
    d. Working with responsible institutional officers to develop and deliver adequate training and education for all employees with access to customer information.

B. Security and Privacy Risk Assessments

1. The Program shall identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of the safeguards in place to control those risks.
2. Risk assessments should include consideration of risks in each office that has access to customer information.
3. Risk assessments must be written and include, at a minimum, consideration of the risks in the following areas:
    a. Criteria for the evaluation and categorization of the identified security risks and threats;
    b. Criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls in the context of identified risks and threats; and
    c. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the Program will address the risks.
4. The institution must periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. Such assessments must reassess the sufficiency of safeguards in place to control the risks.

5. The Coordinator must collaborate with the institution's Internal Auditors and/or Compliance Officers to examine the risk assessment documents before the Coordinator submits them to the System Office.

C. Information Security Personnel and Employee Training.

1. Institutions must utilize qualified information security personnel, whether employed by the institution or through vendors, sufficient to manage information security risks and to assist in oversight of the Program. Security personnel must be provided with security updates and training sufficient to address relevant security risks. Institutions must verify that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

2. The Coordinator must provide institutional employees with mandatory security awareness training that is updated as necessary to reflect risks identified by the risk assessment. This training may be developed and implemented in conjunction with vendors, the human resources office, and the Office of General Counsel. The training shall occur on a regular basis, as deemed appropriate by the Coordinator, and it shall include education on relevant policies and procedures and other safeguards in place or developed to protect customer information.

3. Failure to complete the mandatory training will result in the suspension of IT resource access. The Coordinator will establish the procedures for correction and the reinstatement of such privileges.

D. Design and Implementation of Safeguards

1. The Program must include safeguards to control the risks identified through the risk assessments, including by:
    a. Implementing and periodically reviewing access controls, including technical, and as appropriate, physical controls to authenticate and permit access only to authorized users, and to limit authorized users' access only to customer information that they need to perform their duties and functions (or in the case of customers, to access their own information);
    b. Identifying and managing the data, personnel, devices, systems, and facilities that enable the institution to achieve operational purposes in accordance with their relative importance to operational objectives and risk strategy;
    c. Protecting by encryption all customer information held or transmitted by the institution both in transit over external networks and at rest. To the extent the Coordinator determines that encryption of customer information, either in transit or at rest, is infeasible, the Coordinator may approve a method to secure such customer information using effective alternative compensating controls;
    d. Adopting secure development practices for in-house developed applications used to transmit, access, or store customer information and procedures to evaluate, assess, or test the security of externally developed applications used to transmit, access, or store customer information;
    e. Implementing multi-factor authentication for any individual accessing any information system, unless the Coordinator

has approved in writing the use of reasonably equivalent or more secure access controls;

f. Developing, implementing, and maintaining procedures for the secure disposal of customer information. These procedures must be periodically reviewed to minimize the unnecessary retention of data. Disposal must occur no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates unless:

(1) The information is required to be kept for a longer period in accordance with TBR Policy 1.12.01.00, Records Retention and Disposal of Records;

(2) The information is necessary for operational purposes; or

(3) Targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

g. Implementing immutable or air gapped backups to safeguard campus data from potential threats or accidental deletions;

h. Implementing Endpoint Detection and Response (EDR) software on all college-owned endpoints;

i. Implementing guidelines for evaluation and acquisition of technology;

j. Adopting procedures for change management; and

k. Implementing policies, procedures, and controls designed to monitor and log the activity of authorized users and to detect unauthorized access or use of, or tampering with, customer information by such users.

2. The Program must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

3. For information systems, monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments. In the absence of effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, the institution must conduct:

    a. Annual penetration testing of information systems based on relevant risks identified through risk assessments; and

    b. Vulnerability assessments, including any systemic scans or reviews of information systems designed to identify publicly known security vulnerabilities. Such vulnerability assessments must be conducted at least every six months and whenever there are material changes to an institution's operations, and when circumstances or events may have a material impact on the Program.

E. Oversight of Service Providers and Contracts

1. The institution must take reasonable steps to select and retain third party service providers that are capable of maintaining appropriate safeguards for the customer information to which they have access. Service providers must be periodically assessed based on the risk they present and the continued adequacy of their safeguards.

2. The institution must require, by contract, that current and potential service providers with access to customer information maintain sufficient procedures to detect and respond to security events.
3. The institution must require, by contract, that all applicable third party service providers implement and maintain appropriate safeguards for customer information.
4. The institution must require, by contract, that any vendor that accesses and/or stores sensitive institutional data shall at a minimum provide documented assurance of their compliance of their security and privacy controls.

F. Incident Response Plan

1. The Program must include a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in the institution's control.
2. To the extent the following requirements are not already required by the State of Tennessee's incident response plan, the Coordinator shall ensure that the incident response plan addresses:
    a. The goals of the incident response plan;
    b. The internal processes for responding to a security event;
    c. The definition of clear roles, responsibilities, and levels of decision-making authority;
    d. External and internal communications and information sharing;
    e. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

f. Documentation and reporting of security events and related incident response activities; and

g. The evaluation and revision as necessary of the incident response plan following a security event.

G. Evaluation and Revision of Program

1. The Coordinator must evaluate and adjust the Program in light of the results of testing and monitoring, any material changes to the institution's operations, the results of risk assessments, and any other circumstances that may have a material impact on the Program.

2. The Program must include a plan by which it will be evaluated on a regular basis and a method to revise the Program, as necessary, for continued effectiveness.

3. The Program must also include the requirements of ensuring that the incident response plan meets current requirements of the State of Tennessee's cyber insurance policy and sending the current incident response plan to the System Office and Treasury annually.

III. Assessment of the Information Security Program

A. The Coordinator, in conjunction with the appropriate administrators, shall assess the effectiveness of the Program annually.

B. The Coordinator shall make certain that necessary revisions to the Program are made at the time of the annual review to address any changes in the institutional organization that may affect the implementation and effectiveness of the Program.

IV. Publication of the Information Security Program

A. To promote uniform compliance with the Program by all personnel employed by the institution and to achieve the institution's duty to safeguard the confidentiality of customer information, the institution shall, at a minimum, display and disseminate the Program in accordance with the institution's standard distribution methods.

B. The institution's current Program shall be available upon request for review and copy at all times.

V. Annual Reporting to the Board of Regents

A. The System Office Coordinator shall provide a written report to the Board of Regents no less than annually. The report shall include the following information for the System Office and TCATs:

1. The overall status of the Program and compliance with these guidelines; and

2. Material matters related to the Program addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and responses thereto; and recommendations for changes to the Program.

B. The System Office Coordinator's report to the Board of Regents shall also include a report from Coordinator of each institution. The System Office Coordinator shall prepare a form for institutional Coordinators to complete and return in time sufficient for inclusion in the report to the Board.

Sources

Authority

T.C.A. § 49-8-203; All state and federal statutes, codes, Acts, rules and regulations referenced in this guideline; 16 C.F.R. Part 314.

This guideline is aligned with the requirements of the Gramm-Leach-Bliley Act (GLBA) and the National Institute of Standards and Technology (NIST) Special Publication 800-171, which provide guidelines for protecting the confidentiality of sensitive customer and institutional data.

History

November 5, 2003; Revision Approved at Presidents Meeting February 22, 2023.

B-090 Safeguarding Nonpublic Financial Information

Policy/Guideline Area

Business and Finance Guidelines

Applicable Divisions

TCATs, Community Colleges, System Office

Purpose

This guideline explains the procedure by which Tennessee Board of Regents institutions must develop a comprehensive written Information Security Program (the "Program") as mandated by the Gramm-Leach-Bliley Act ("GLBA") Standards for Safeguarding Customer Information Rule. An institution's Program must include the components described below pursuant to which the institution intends to:

1. Protect the security and confidentiality of customers' nonpublic financial information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

The Program may consist of existing institutional policies and procedures that are incorporated by reference into the Program, including but not limited to policies such as computer/electronic records confidentiality policies, Family Educational Rights & Privacy Act policies, employee/personnel records confidentiality policies, etc.

Definitions

- Customer - person who has a continuing relationship with the institution for provision of financial services, such as financial aid.
- Customer Information - any record containing nonpublic personal financial information about a Customer.
- Non-public financial information – any record not publicly available that an institution obtains about a customer in the process of offering a financial product or service, as well as such information provided to the institution by another

source. Nonpublic financial information includes information that a person submits to apply for financial aid (e.g., tax returns and other financial information), that an institution collects from third parties relating to financial aid (e.g., FAFSA information), and that an institution creates based on customer information in its possession.

- Security event – an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

Policy/Guideline

I. Introduction

A. TBR institutions are covered by GLBA because they offer and process financial aid applications, provide loans to students, and receive customer information from students and others in connection with those activities.

B. Each institution must develop, implement, and maintain a written, comprehensive Information Security Program. The Program must contain administrative, technical, and physical safeguards appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. The Program must apply to any paper or electronic record maintained by an institution that contains customer information about an individual or a third party who has a relationship with the institution.

C. Because the TBR System Office handles significant customer information for Tennessee Colleges of Applied Technology through Shared Services, the System Office and the TCATs are considered a single institution for purposes of this policy. Customer information shall be kept confidential and safeguarded by the institution, its affiliates and service providers pursuant to the provisions of the Program and this Guideline.

II. Requirements of an Information Security Program

A. Program Coordinator

1. Except for the TCATs, which will be served by the TBR System Office Program Coordinator, each institution must identify one qualified individual to serve as the Program Coordinator ("Coordinator") who shall be responsible for overseeing and implementing the Program. The Coordinator may obtain assistance from other sources, but ultimate responsibility for the Program remains with the Coordinator.
2. The Coordinator's development of the Program shall include, but not be limited to:
    a. Consulting with the appropriate offices to identify units and areas of the institution with access to customer information and maintaining a list of the same;
    b. Assisting the appropriate offices of the institution in identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and making certain that appropriate safeguards are designed and implemented in each office and throughout the institution to safeguard the protected data
    c. Working with the institution's contract officer(s) to guarantee that all contracts with third party service providers that have access to and maintain customer information include a provision requiring that the service provider maintain appropriate safeguards for customer information; and
    d. Working with responsible institutional officers to develop and deliver adequate training and education for all employees with access to customer information.

B. Security and Privacy Risk Assessments

1. The Program shall identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of the safeguards in place to control those risks.
2. Risk assessments should include consideration of risks in each office that has access to customer information.
3. Risk assessments must be written and include, at a minimum, consideration of the risks in the following areas:
    a. Criteria for the evaluation and categorization of the identified security risks and threats;
    b. Criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls in the context of identified risks and threats; and
    c. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the Program will address the risks.
4. The institution must periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. Such assessments must reassess the sufficiency of safeguards in place to control the risks.

5. The Coordinator must c~~C~~ollaborate with the institution's Internal Auditors and/or Compliance Officers to examine the risk assessment documents before the Coordinator ~~they are~~ submit~~sted~~ them to the System Office.

C. Information Security Personnel and Employee Training.

1. Institutions must utilize qualified information security personnel, whether employed by the institution or through vendors, sufficient to manage information security risks and to assist in oversight of the Program. Security personnel must be provided with security updates and training sufficient to address relevant security risks. Institutions must verify that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

2. The Coordinator must provide institutional employees with mandatory security awareness training that is updated as necessary to reflect risks identified by the risk assessment. This training may be developed and implemented in conjunction with vendors, the human resources office, and the Office of General Counsel. The training shall occur on a regular basis, as deemed appropriate by the Coordinator, and it shall include education on relevant policies and procedures and other safeguards in place or developed to protect customer information.

3. Failure to complete the mandatory training will result in the suspension of IT resource access. The ~~campus~~ Coordinator will establish the procedures for correction and the reinstatement of such privileges.

D. Design and Implementation of Safeguards

1. The Program must include safeguards to control the risks identified through the risk assessments, including by:
    a. Implementing and periodically reviewing access controls, including technical, and as appropriate, physical controls to authenticate and permit access only to authorized users, and to limit authorized users' access only to customer information that they need to perform their duties and functions (or in the case of customers, to access their own information);
    b. Identifying and managing the data, personnel, devices, systems, and facilities that enable the institution to achieve operational purposes in accordance with their relative importance to operational objectives and risk strategy;
    c. Protecting by encryption all customer information held or transmitted by the institution both in transit over external networks and at rest. To the extent the Coordinator determines that encryption of customer information, either in transit or at rest, is infeasible, the Coordinator may approve a method to secure such customer information using effective alternative compensating controls;
    d. Adopting secure development practices for in-house developed applications used to transmit, access, or store customer information and procedures to evaluate, assess, or test the security of externally developed applications used to transmit, access, or store customer information;
    e. Implementing multi-factor authentication for any individual accessing any information system, unless the Coordinator

has approved in writing the use of reasonably equivalent or more secure access controls;

f. Developing, implementing, and maintaining procedures for the secure disposal of customer information. These procedures must be periodically reviewed to minimize the unnecessary retention of data. Disposal must occur no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates unless:

(1) The information is required to be kept for a longer period in accordance with TBR Policy 1.12.01.00, Records Retention and Disposal of Records;

(2) The information is necessary for operational purposes; or

(3) Targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

g. Implementing immutable or air gapped backups to safeguard campus data from potential threats or accidental deletions;~~.~~

h. Implementing Endpoint Detection and Response (EDR) software on all ~~campus~~ college-owned endpoints~~.~~;

i. Implementing guidelines for evaluation and acquisition of technology;~~.~~

~~g.~~j. Adopting procedures for change management; and

~~h.~~k. Implementing policies, procedures, and controls designed to monitor and log the activity of authorized users and to detect unauthorized access or use of, or tampering with, customer information by such users.

2. The Program must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

3. For information systems, monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments. In the absence of effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, the institution must conduct:

    a. Annual penetration testing of information systems based on relevant risks identified through risk assessments; and

    b. Vulnerability assessments, including any systemic scans or reviews of information systems designed to identify publicly known security vulnerabilities. Such vulnerability assessments must be conducted at least every six months and whenever there are material changes to an institution's operations, and when circumstances or events may have a material impact on the Program.

E. Oversight of Service Providers and Contracts

1. The institution must take reasonable steps to select and retain third party service providers that are capable of maintaining appropriate safeguards for the customer information to which they have access. Service providers must be periodically assessed based on the risk they present and the continued adequacy of their safeguards.

2. The institution must require, by contract, that current and potential service providers with access to customer information maintain sufficient procedures to detect and respond to security events.

3. The institution must require, by contract, that all applicable third party service providers implement and maintain appropriate safeguards for customer information.

~~3.~~4. The institution must require, by contract, that any vendor that accesses and/~~-~~or stores sensitive institutional data shall at a minimum provide documented assurance of their compliance of their security and privacy controls.

F. Incident Response Plan

1. The Program must include a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in the institution's control.

2. To the extent the following requirements are not already required by the State of Tennessee's incident response plan, the Coordinator shall ensure that the incident response plan addresses:

   a. The goals of the incident response plan;

   b. The internal processes for responding to a security event;

   c. The definition of clear roles, responsibilities, and levels of decision-making authority;

   d. External and internal communications and information sharing;

   e. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

f. Documentation and reporting of security events and related incident response activities; and

g. The evaluation and revision as necessary of the incident response plan following a security event.

G. Evaluation and Revision of Program

1. The Coordinator must evaluate and adjust the Program in light of the results of testing and monitoring, any material changes to the institution's operations, the results of risk assessments, and any other circumstances that may have a material impact on the Program.

2. The Program must include a plan by which it will be evaluated on a regular basis and a method to revise the Program, as necessary, for continued effectiveness.

~~2.~~3. The Program must also include the requirements of ensuring that the incident response plan meets current requirements of the State of Tennessee's cyber insurance policy and sending the current incident response plan to the System Office and Treasury annually. ~~This will ensure that the institution is in compliance with the state and receives the discounted cyber insurance policy.~~

III. Assessment of the Information Security Program

A. The Coordinator, in conjunction with the appropriate administrators, shall assess the effectiveness of the Program annually.

B. The Coordinator shall make certain that necessary revisions to the Program are made at the time of the annual review to address any changes in the institutional organization that may affect the implementation and effectiveness of the Program.

IV. Publication of the Information Security Program

A. To promote uniform compliance with the Program by all personnel employed by the institution and to achieve the institution's duty to safeguard the confidentiality of customer information, the institution shall, at a minimum, display and disseminate the Program in accordance with the institution's standard distribution methods.

B. The institution's current Program shall be available upon request for review and copy at all times.

V. Annual Reporting to the Board of Regents

A. The System Office Coordinator shall provide a written report to the Board of Regents no less than annually. The report shall include the following information for the System Office and TCATs:

1. The overall status of the Program and compliance with these guidelines; and

2. Material matters related to the Program addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and responses thereto; and recommendations for changes to the Program.

B. The System Office Coordinator's report to the Board of Regents shall also include a report from Coordinator of each institution. The System Office Coordinator shall prepare a form for institutional Coordinators to complete and return in time sufficient for inclusion in the report to the Board.

Sources

Authority

T.C.A. § 49-8-203; All state and federal statutes, codes, Acts, rules and regulations referenced in this guideline; 16 C.F.R. Part 314.

This guideline is aligned with the requirements of the Gramm-Leach-Bliley Act (GLBA) and the National Institute of Standards and Technology (NIST) Special Publication 800-171, which provide guidelines for protecting the confidentiality of sensitive customer and institutional data.

History

November 5, 2003; Revision Approved at Presidents Meeting February 22, 2023.

THE COLLEGE SYSTEM of TENNESSEE

Presidents Quarterly Meeting
August 7, 2024

SUBJECT:	Digital Identity Authentication Management and Access Control Policy
PRESENTER:	Jon Calisi
LENGTH OF PRESENTATION:	*(5 minutes)*
ACTION REQUIRED:	Requires Vote

Summary:

The purpose of this policy is to establish a minimum expectation with respect to digital identity authentication methods, access controls, and password construction to protect data stored on computer systems throughout the TBR system.

Merged content from the previous Access Control policies G-051 and G-052 into policy 1.08.02.00 to eliminate redundant wording and enhance the existing policy.

The proposed revisions, which have been approved by the IT Sub council, are attached in tracked changes and clean copy form.

Digital Identity, Authentication Management, and Access Control: 1:08:02:00

Policy Area
General Policy

Applicable Divisions
TCATs, Community Colleges, System Office, Board Members

Purpose
The purpose of this policy is to establish a minimum expectation with respect to digital identity authentication methods, access controls, and password construction to protect data stored on computer systems throughout the TBR system.

Policy

I. Secure Authentication Methods

Secure methods that uniquely identify the user shall be used for authentication of access to all TBR and institutional networks and systems. Examples of secure authentication methods include passwords, two-factor authentication (2FA), biometrics, and public/private key pairs.

II. Password (and Passphrase) Construction

a) To safeguard institutional data access, it's essential to establish and maintain robust password management protocols. All users are obliged to create secure passwords for network and system access in alignment with the given guidelines (except when technological limitations prevent adherence):
b) Instead of conventional passwords, passphrases may be utilized. Passphrases are exempt from complexity regulations.
c) Both passwords and or passphrases shall be at least 14 characters long at a minimum.
d) Passwords should include at least three out of the following four character types:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Special characters or symbols (when allowed by the software)

III. Password Management

1. Storage and Visibility

a) Passwords must not be stored in a manner which allows unauthorized access.

b) Passwords will not be stored in a clear text file.
c) Passwords will not be sent via unencrypted e-mail.

2. Changing Passwords

a) If 14-character passwords or longer and or passphrases are used, there is no requirement for routine password expiration/rotation. Otherwise, users must change their passwords every 120 days.
b) Passwords must be changed within one business day if any of the following events occur:
    - Unauthorized password discovery or usage by another person
    - System compromise (unauthorized access to a system or account)
    - Insecure transmission of a password
    - Accidental disclosure of a password to an unauthorized person
    - Status changes for personnel with access to privileged and/or system accounts
c) Password Files and Hashes
    - Password files or hashes should not be shared with any entity without formal written consent.

3. System Accounts

1. System accounts are not required to expire but must meet the password construction requirements above (where supported by the underlying technologies).
2. Vendor-provided passwords must be changed upon installation using the password construction requirements above (where supported by the underlying technologies).

IV. Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is required to be used by all users with public-facing access to critical systems such as information systems, email, or remote access such as virtual private networks (VPN).

V. Access Controls

a) Access to information assets must be restricted to authorized users and must be protected by appropriate physical, administrative, and logical authentication and authorization controls.
b) Protection for information assets must be commensurate with the

classification level assigned to the information.

c) Each computer system shall have an automated access control process that identifies and authenticates users and then permits access based on defined requirements or permissions for the user or user type.
d) All users of secure systems must be accurately identified; a positive identification must be maintained throughout the login session, and actions must be linked to specific users.
e) Access control mechanisms may include user IDs, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

VI. Access Privileges

a) Each user's access privileges shall be authorized on a need-to-know basis as dictated by the user's specific and authorized role.
b) Authorized access shall be based on least privilege, meaning only the minimum privileges required to fulfill the user's role shall be permitted.
c) Access privileges shall be defined to maintain appropriate segregation of duties to reduce the risk of misuse of information assets.
d) Any access granted to data must be authorized by the appropriate data trustee.
e) Access privileges shall be controlled based on the following criteria as appropriate:
    - Identity (user ID)
    - Role or function
    - Physical or logical locations
    - Time of day/week/month
    - Transaction-based access
    - Access modes such as read, write, execute, delete, create, and/or search
f) Privileged access (e.g., administrative accounts, root accounts) must be granted based strictly on role requirements.
g) The number of personnel with special privileges should be carefully limited.

VII. Access Account Management

a) User ID accounts must be established, managed, and terminated to maintain the necessary level of data protection.
b) The following requirements apply to network logons as well as individual application and system logons and should be implemented where technically and procedurally feasible:

- Account creation requests must specify access either explicitly or request a role that has been mapped to the required access.
- New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights.
- Accounts must be locked out according to individual campus requirements after an institution-defined number of consecutive invalid logon attempts.
- When a user account is locked out, it should remain locked out for a minimum of five minutes or until authorized personnel unlock the account.
- User interfaces must be locked according to individual campus requirements after an institution-defined length of system/session idle time.
    - This requirement applies to workstation and laptop sessions as well as application sessions where feasible.
    - The office of information technology shall implement measures to enforce this requirement and to require the user to re-authenticate to reestablish the session.
- Systems housing or using restricted information must be configured in such a way that access to the restricted information is denied unless specific access is granted.
- Access to restricted information is never to be allowed by default.
- Information Technology personnel revoke access upon notification that access is no longer required in accordance with the following procedures:
    - Access privileges of terminated or transferred users must be revoked or changed as soon as notification of termination or transfer occurs.
    - In cases where an employee is not leaving on good terms, the user ID must be disabled simultaneously with departure.
    - Access for users who are on leaves of absence or extended disability must be suspended until the user returns.
    - Access to Banner Admin Pages is consistently denied to adjunct faculty members. The procedure for managing access for adjunct faculty accounts is established at the local institution level, incorporating defined dates of employment according to contract status and integrating input from entities responsible for adjunct contract oversight. Each institution, guided by its academic calendar and directives from contract control authorities for adjunct faculty, will implement this specified procedure on a schedule set by the respective campus. The

scope of this process is to be defined by each individual campus, ensuring that adjunct faculty have restricted access beyond their designated course timelines to fulfill job requirements, which may be extended upon a justified request detailing specific access needs.

- User IDs will be disabled after a period of inactivity that is determined appropriate by the current business process and the individual campus.
- All third-party access (contractors, business partners, consultants, vendors) must be authorized and monitored using processes determined by the individual campuses.
- Appropriate logging will be implemented commensurate with the sensitivity/criticality of the data and resources.
- Logging of attempted access must include failed logons.
- Where practical, successful logons to systems with restricted information shall be logged.
- Logs should be monitored and regularly reviewed to identify security breaches or unauthorized activity.
- Logs shall be maintained for at least ninety days.
- A periodic audit of secured systems to confirm that access privileges are appropriate must be conducted. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.
- Applications requiring an account not tied to a single user shall employ service-based accounts. Users oversee these accounts and maintain their passwords.
- Applications requiring these accounts shall be monitored and audited by individual campus documented procedures dictated by the application for which they are provisioned.
- Service-based accounts due to their application-centric use are not subject to standard user account management rules.

VIII. Compliance and Enforcement

a) The policy applies to all users of information resources, including students, faculty, staff, temporary workers, vendors, and any other authorized users.
b) Persons in violation of this policy are subject to a range of sanctions determined and enforced by the individual institutions, including the loss of computer network access privileges, disciplinary action, dismissal from the institution, and legal action.

c) Some violations may constitute criminal offenses per Tennessee and other local and federal laws. The institution will carry out its responsibility to report such violations to the appropriate authorities.
d) Documented exceptions to this policy may be granted by the information security officer for the institution based on limitations to risk and use.

Definitions

Authentication: A process that allows a device or system to verify the unique identity of a person, device, or other system that is requesting access to a resource.

Digital identity: Information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. Also referred to as a user account or user profile.

System account: A special account used for automated processes without user interaction or for device management. These accounts are not assigned to an individual user for login purposes.

Privileged account: An account with elevated access or privileges to a secure system or resource. This type of account is authorized and trusted to perform security-relevant functions that an ordinary user account is not authorized to perform. Privileged accounts are assigned to individual users. The College System of Tennessee – the system office and affiliated institutions

References

NIST Special Publication 800-63: Digital Identity Guidelines Frequently Asked Questions

History

Merged content from the previous Access Control policies G-051 and G-052 into policy 1.08.02.00 to eliminate redundant wording and enhance the existing policy.