BUSINESS AFFAIRS SUB-COUNCIL

July 26, 2016

MINUTES

The meeting began at 9:00 a.m. in the TBR Board Room. Present were Mr. Tim Amyx (VSCC); Ms. Cynthia Brooks (TSU); Mr. Steve Campbell (NeSCC); Mr. Horace Chase (JSCC); Dr. David Collins (ETSU); Ms. Beth Cooksey (VSCC); Ms. Mary Cross (NaSCC); Ms. Elaine Curtis (CoSCC); Ms. Alisha Fox (ClSCC); Mr. Danny Gibbs (RSCC); Mr. Lowell Hoffman (DSCC); Mr. Mark Hurst (WSCC); Mr. Ron Kesterson (PSCC); Ms. Laura Moran (NaSCC); Mr. Mitch Robinson (APSU); Ms. Jeannie Smith (UOM); Dr. Claire Stinson (TTU); Ms. Tammy Swenson (ChSCC); Mr. Alan Thomas (MTSU); Ms. Kathy Thurman (MTSU); Ms. Hilda Tunstill (MSCC); Mr. Greg Wilgocki (ETSU); Mr. Jeff Young (TTU); Mr. David Zettergren (UOM); Ms. Tammy Birchett, Ms. Angela Flynn, Ms. Alicia Gillespie, Ms. Deanna Hall, Ms. Lisa Hall, Ms. Ginger Hausser, Ms. Denise Lawrence, Ms. Pat Massey, Dr. Warren Nichols. Ms. April Preston, Mr. Wayne Pugh, Ms. Brooke Shelton, Mr. Dale Sims, Ms. Renee Stewart, Mr. Stephen Vieira and Mr. Bob Wallace (TBR).

1. **Facilities Management Outsourcing**

   Dr. Nichols updated the committee on the status of the facilities management outsourcing initiative. The RFQ has been issued but no decisions have been made at this point in time. Based on information gathered from the RFQ, it appears that if an institution does elect to go with an outside agency, they will have the ability to opt-in or out of certain services. If institutions choose to go through with the outsourcing, one of the issues that will need to be addressed is how to handle possible transition of employees and their benefits. Institutions were again reminded to evaluate their spending compared to the Whitestone Benchmark to aid in their decision making.

2. **Chancellor's Remarks**

   The Chancellor updated the committee on the FOCUS Act. The universities must submit a prospectus to the SACS committee by September, for their December meeting. The universities will submit their applications for substantive change and accreditation simultaneously. Normally, SACS requires that a substantive change be implemented within 30 days, so an exception will be needed due to the timeline of the proposed changes. However, this does not appear to be a barrier to approval.

   The Chancellor also discussed the timeline of the FOCUS Act transition and training. The governor will make nominations of university board members in September. These recommendations will be confirmed during the 2017 legislative session around February or March. Once confirmed, the university board members will begin receiving training by THEC in March or April 2017. It was also brought to the attention of the group that THEC plans to issue non-binding tuition guidance in the fall, and then issuing the binding recommendations in March or April. This means that the new board members would be

asked to set tuition at their first meeting. A recommendation was made to allow the universities to begin working with their board members on this issue as soon as they are confirmed.

3. Cyber Incident Response Plan

On June 27, 2016, a meeting was held with representatives from Treasury-Risk Management concerning the cyber incident response plan. Mr. Vieira reminded the committee that this was meant to be used if/when an incident occurs and it is not designed to prevent an incident from occurring. He has stressed to the IT Sub-Council that any incidents should be reported to TBR first, and TBR staff will route them through the proper channels. He is also collecting the previously submitted institutional plans and combining the best aspects of each to create a cyber incident response plan for TBR. Mr. Vieira also plans to develop a portal or reporting template so that when an incident does occur, it can be reported online where it can be more easily tracked and used as a reference on how to prevent future incidents. (Attachment A)

4. Residency Requirements Proposal

Mr. Amyx and Ms. Moran presented a proposed business process document that will help provide consistency among community colleges regarding the determination of in-state residency status for students. Community college admissions directors worked together and unanimously voted to approve the document. It was noted that this is not a policy or guideline, but a business process document that will establish a minimum baseline for institutions to use when determining residency status. The document does allow flexibility for an institution to make judgement calls for instances that are not covered. (Attachment B)

5. <u>Report of the Committees</u>

A. Finance Committee

Dr. Collins highlighted the following issues from the July 12, 2016 Finance Committee meeting:

- Study Abroad Procedures

  The committee discussed the proposed study abroad business guideline. It had been previously discussed to record the program fee revenue and related expenses in an agency fund account specific to the responsible program or office. Any student-specific expenses such as travel, lodging, tours, or supplies would also be paid from the agency account.

  After further discussion, the committee determined that institutions running their own study abroad programs should record the fee revenue and related expenses in an E&G account. This would not apply to third party programs, such as TNCIS.

Institutions using third party programs would still need to record those revenues and expenses in an agency account. (Attachment C)

- Foundation Policy Agreement

  The committee discussed the new foundation policy agreement adopted by the Board last year, in which the institutions were given a year to adopt the new agreement. A reminder will be sent to the institutions that a signed and fully executed copy is due September 30.

The Finance Committee minutes were approved.

B. Council of Buyers

Ms. Flynn highlighted the following issues from the June 23, 2016 Council of Buyers meeting:

- DocuSign

  TBR is in the process of implementing DocuSign for automated workflows and approvals. The TBR System Office will be implementing the use of DocuSign in a tiered structure during the month of July for procurement and contract requests/approvals.

  A system-wide training webinar was held on July 20, 2016, to instruct institutions how to submit to the TBR System Office for approval. Beginning August 1, 2016, institutions are to begin submitting procurement and contract documents to the System Office via DocuSign.

  TBR Purchasing and Contracts will have dedicated space on its webpage for the appropriate forms and training materials to assist users in processing via DocuSign. All documentation will be attached electronically and the actual contract should be in Word version, with no signatures. Once the TBR System Office routing and approval is complete, the TBR Purchasing and Contracts Office will send to both the vendor and institution for signatures. Institutions will have to provide the signatory names and email address to the System Office so that the electronic signatures can be requested and acquired. Because TBR is charged on a per envelope basis, it will be important that the documents put into DocuSign for processing are the final documents that conform to all state laws, policies and guidelines.

- TSM

  Ms. Flynn updated the committee on the status of the TSM project. The project is now in a "soft, go-live" phase, where institutions are working on the manual changes that they have been tracking. Within the next week, the project is expected to go-live with the vendor community.

- Athletic Insurance Update

  Currently three institutions (RSCC, ClSCC and ChSCC) are using McCloskey to perform administrative services for the insurance program. At this point, everything seems to be going well with the service. Institutions pay a $1,000 fee for McCloskey to administer all claims, and McCloskey claims that they will be able to save institutions at least $1,000 by negotiating claims down.

- PCard Policy and Guideline

  Ms. Flynn informed the group that the proposed PCard policy and guideline has now been before all of the sub-councils. She has received a few remarks, which have now been incorporated into the documents. (Attachments D-J)

- PCard RFP

  TBR has partnered with the State and UT on an RFP for PCard services. It appears that the successful vendor is U.S. Bank. However, negotiations are just now beginning with the provider. It seems that we will be able to get a much better rebate than we have in the past.

  Three institutions and the System Office can move to the contract immediately. Three other institutions are currently under contract with U.S. Bank, so TBR Purchasing and Contracts will work with U.S. Bank to re-negotiate their terms to bring them current with the new contract. All other institutions may join the contract when their current contracts expire.

- Touchnet

  TBR sent out an inquiry several months ago, because our current contract expires in November. TBR, along with UT, will be going to Fiscal Review in September to ask for a new five-year agreement. Given our timeframe, the contract will need to be extended for at least another a year.

  Under the current contract, there is a 4% annual escalator and we have been able to negotiate them down to a 3% escalator going forward. We are looking to extend the contract based on feedback received from institutions who would rather not change vendors due to the complexity involved.

The Council of Buyers minutes, with the policy and guideline changes, were approved.

C. Human Resource Officers

Ms. Preston highlighted the following issues from the July 20, 2016 Human Resource Officers meeting:

- DocuSign

  Ms. Preston informed the group that the Human Resource Officers have also had a training webinar on the use of DocuSign. The electronic process shall be used for all applicable requests to interview and offer, which require TBR System Office review and approval. This process began, effective July 20, 2016.

- Compensation Guidelines

  The compensation guidelines have been distributed to the institutions and are due back to the System Office by August 15, 2016. This year institutions have several options, including the option of adding new positions. Since some institutions will base their compensation changes on enrollment numbers, Ms. Preston asked that the institution go ahead and submit a proposal for both scenarios. This will allow the System Office to simply remove the proposal that is not applicable before the Board meeting.

- Employment Application Process Change

  Effective July 1, 2016, employers can no longer inquire about criminal history on an initial application, unless required by state or federal law. There are three questions regarding criminal history on the TBR system applications. The first two questions must be removed. However, the third question will remain due to state law (TCA Title 40, Chapter 39, Part 2). Our proposal is to leave question three and add an auto email to be sent to those selected for interview. Candidates would click the link in the email to answer the two questions related to felony and misdemeanor convictions, with their interview contingent on answering the questions. However, using this process means the position cannot be closed until those selected for interview have uploaded the additional material. While universities may develop different processes, all community colleges must have the same process, as they use the same electronic application template.

- Changes to Fair Labor Standards Act

  The new salary threshold for FLSA is $47,476. The duties test also applies to the FLSA changes. Full-time teachers and academic administrative positions, meaning those who work with students outside of the classroom in an academic capacity, are exempt. Institutions should assess the salaries and review the job descriptions for the exempt positions that are between the current threshold of $23,660 and the new $47,476.

  Related to possible benefit changes, the ORP election is irrevocable, so if an exempt position is made non-exempt, the employee must remain in the ORP. The leave accrual will be the potential benefit change.

The Human Resource Officers minutes were approved.

D. Internal Audit

Ms. Birchett highlighted the following issues from the July 14, 2016 Internal Audit meeting:

- IT Audits and General Controls Recommendations

  The committee was given an overview of the IT general controls reviews completed by SWIA. A summary of recommendations made and the current status of those items was provided. Some of the recommendations have taken the institutions longer to address, including segments of policies and procedures, an asset management process, a logical process for individual access rights, logging and monitoring of IT activity and the Business Continuity Plan. It was noted that the FY 2017 information systems audit plan would primarily include reviews regarding security and may include social engineering tests as requested. (Attachment K)

- Risk Assessments

  Ms. Birchett reminded the committee that next year begins the new cycle of major processes for Risk Assessment. She encouraged the group to contact her with any recommendations for next year's review.

The Internal Audit Directors minutes were approved.

E. IT Sub-Council

Mr. Vieira highlighted the following issues from the IT Sub-Council meeting:

- There is a new contract for an on-demand library of all training materials offered through Ellucian.
- Oracle 12 G training will be August 15-19, 2016.
- There is now an IT project website within the TBR website that is updated every two weeks.
- The Luminis support project is now live at three institutions, with more coming up in September. The plan is to bring up three institutions at a time, every two weeks to meet the December completion date.
- TBR IT is currently reviewing all 123 modifications made to Banner. Of those, 106 are reports and do not need to be addressed at this time. Ten of them will be taken into account when moving to Banner XE. That leaves seven that need to be looked at as they try to get back to a baseline Banner instance before the upgrade to Banner XE. IT is currently working with Ellucian to provide us with a free fit-gap analysis of how these could be imbedded into Banner.
- The TN Summit will be held at MTSU October 10-11, 2016.

6. Legislative Update

Ms. Hausser informed the committee that there is now a dedicated FOCUS section on the TBR website at: https://www.tbr.edu/focus/focus-act. The website is frequently updated with information pertaining to the act, such as the timeline, key components, questions and answers, and a legislative compilation.

7. G-050 Enterprise Information Systems Update

The policy originally stated that institutions should not be more than one version behind the current release. This policy has now been updated to state that institutions should not be more than one version behind the current "ERP vendor-certified release". (Attachment L)

9. G-051 Password Management

This guideline is currently under review by the IT Sub-Council. There seems to be issues with some institutions' software that does not allow them to maintain the password requirements in the guideline. The Sub-Council will review and make modifications to the guideline if necessary.

10. Mod Review

IT is reviewing the 123 Banner modifications to see if any of them can be imbedded into Banner. A MOU was issued some time ago saying that Ellucian would look into this, but that has not happened yet. It is the hope of IT that between the MOU, Ellucian fit-gap analysis and a report from UOM a few years ago, they will be able to minimalize the number of mods remaining. Mr. Vieira also discussed having conversations with UT Martin to see how they are preforming using Banner with no mods.

10. Deferred Payment Pilot Plan

Mr. Chase updated the committee on the results of the community college deferred payment pilot program. During the Spring 2016 semester, JSCC implemented a revised payment plan, which increased the number of installment payments to four. The institution saw an increase in both the number and dollar amount of outstanding balances as compared to the previous year. JSCC will offer the plan again for the Fall semester, and make a recommendation on whether or not to proceed in the Spring of 2017 based on the results.

There being no further business, the meeting was adjourned at 11:11 a.m.

Attachment A

CYBER INCIDENT RESPONSE PLAN

[Cover]

Agency
Incident Response Plan

EXAMPLE ONLY

Cloud services…Deductible…

Prepared by:
State of Tennessee, Treasury Department
Division of Risk Management Claims Administration
[Date]

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The State of Tennessee, Treasury Department, Division of Risk Management and Claims Administration, has purchased Cyber Liability Insurance Coverage to protect State Agencies and Departments. In order to ensure coverage under this policy, each agency must implement a cyber-incident response plan. The Treasury Department has developed the following Cyber Incident Response Plan (CIRP) as a guide and framework to be used in the event of a cyber-incident. This CIRP guide is designed to assist with tailoring your own CIRP for the purpose of meeting the specific operational needs for your organization.

Cyber incidents can be accidental or malicious actions or events that have the potential of causing unwanted effects on the confidentiality, integrity and availability of State information and IT assets. Cyber incidents include, but not limited to, theft or loss of physical equipment, illegal access to systems or information, and failing to protect and secure electronic Personal Identifiable Information (PII) and/or Personal Health Information (PHI). These situations can cause your agency or department to face unnecessary expense in productivity, significant damage to systems and damage to your agency or department's reputation. Clearly, the need now exists to take action prior to suffering the consequences of a serious computer security issue.

The goal of the State of Tennessee's CIRP is to assist agencies and departments with managing a cyber-security event or incident for the purpose of mitigating damages, increasing the confidence and trust of all stakeholders and to reduce the recovery time and costs of a cyber-security breach. The CIRP will assist with decision making, internal and external coordination, unity of effort, and minimization of reputational and financial losses for your organization. This will be achieved through the implementation of these procedures outlined within this plan. The CIRP provides operational instructions for the discovery of a cyber-breach, the investigation and remediation process, the assembly of the internal response team, determining the escalation level, contacting law enforcement, the utilization of vendors, the notification process, establishing a call center and post incident lessons learned.

Effective planning must incorporate coordination across all business functions, for example, organizational communications among leadership, regulatory affairs, legal, compliance and audit and operational functions. Internal coordination, combined with easily accessible documentation of CIRP, ensures that all levels of an organization can react with greater alertness during an incident. If your agency discovers a cyber-breach or if you have any questions regarding this CIRP, please contact the Treasury Department, Division of Risk Management and Claims Administration, at 615-741-2734. Additionally, pursuant to Tennessee Code Annotated, Section 8-4-119, your agency is required to notify the Tennessee Comptroller of the Treasury by submitting a report at: http://www.comptroller.tn.gov/DataBreach

Please note that this is a guide and that it is up to the individual State agency or higher learning institution to develop a CIRP that strategically fits the needs of their organizational structure.

Furthermore, there will be mandatory requirements within this guide that SHALL be adopted into your organizations CIRP. These mandatory requirements will be highlighted in "BOLD" type.

STATE OF TENNESSEE, *[NAME OF AGENCY/DEPARTMENT/UNIVERSITY/COLLEGE]*

CYBER INCIDENT RESPONSE PLAN

1.0 INTRODUCTION

1.1 GLOSSARY OF TERMS

TERM	DEFINITION
Advanced Persistent Threat (APT)	An advanced persistent threat is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to your network or organization. An APT uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term.
Breach	The term "breach" is used to include the loss control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where any person that is not authorized and does not have an authorized purpose to have access or potential access to information, whether physical or electronic. It includes both intrusions (from outside the organization) and misuse (from within the organization). Malware infections will be considered a breach ONLY if it is widespread and infects computers where repairs or replacement costs exceed $25,000, or where data is known to have been compromised.
Business Identifiable Information (BII)	Business identifiable information is information about a company or other business entity that could be used to commit or facilitate the commission of fraud, deceptive practices or other crimes. Examples include, but are not limited to, bank account information, trade secrets, and confidential or proprietary business information.
Command Center	For the purposes of this document, the command center is the central point of contact which any member of the respective government sector (STS/UT/TBR) can contact to report a cyber-security incident.

TERM	DEFINITION
Communications Officer/Public Information Officer (PIO)	NA
Computer Security Incident Response Team (CSIRT)	The computer incident response team is comprised of State subject matter experts who provide guidance and advice, and operational employees who undertake the actions required to mitigate the threat and investigate computer security events and incidents. These can be system administrators, database administrators, network engineers, or application administrators/programmers.
Cyber Security Event	A Cyber Security event is an observable change that adversely impacts the established security behavior of an environment or system.
Cyber Security Incident	A cyber security incident can be accidental or malicious actions or events that have the potential of causing actual or potential jeopardy to the confidentiality, integrity, and availability of State data and information technology assets.
Data Exfiltration	Data exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various different techniques, typically by cybercriminals, over the internet or other network.
Denial of Service (DoS)	A DoS is a type of attack that attempts to prevent a system from performing its normal functions or, more frequently attempts to prevent authorized users from accessing a system.
Executive Management TEAM (EMT)	The executive management team is comprised of the senior leadership for the [Name of Agency/Department/ University/ College].
Harm	For the purposes of this document, harm means any adverse effects that would be experienced by an individual or organization (e.g., that may be socially, public trust, physically or financially damaging) whose information was breached, as well as any adverse effects experienced by the organization that maintains the information.

TERM	DEFINITION
Human Resources (HR)	NA
Imminent Threat	Imminent threat is a situation in which the agency has a factual basis for believing that a specific incident is about to occur. For example, the agency receives a bulletin from Microsoft warning of operating system vulnerabilities that must be patched immediately.
Inappropriate Usage	Inappropriate usage entails the use of resources in ways other than their intended purpose or which have not been approved. Examples include, but are not limited to, any illegal use of State computer systems; using State computer systems to conduct personal business, and sending communications that violate established conduct policies.
Incident Lead (IL)	The incident lead is an individual appointed the highest official within in the Executive Management Team to direct and manage the internal response team, as well as to act as the go-between for the Executive Management Team.
Identity Theft	Identity theft is the act of obtaining or using an individual's identifying information without authorization in an attempt to commit or facilitate the commission of fraud or other crimes. The resulting crimes usually occur in one of the following ways. Identity thieves may attempt to: • Gain unauthorized access to existing bank, investment or credit accounts using information associated with the person. • Withdraw or borrow money from existing accounts or charge purchases to the accounts. • Open new accounts with a person's identifiable information without that person's knowledge. • Obtain driver's licenses, social security cards, passports or other identification documents using the stolen identity.
Legal, Audit and Compliance Team	The legal, audit and compliance team is comprised of Agency and Treasury personnel.

TERM	DEFINITION
Malware	Short for malicious software, malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted, and usually harmful, action. Examples include, but are not limited to, worms, viruses, key-loggers, rootkits, and Trojans.
Unauthorized Access	Unauthorized access occurs when individuals or systems are able to access data, resources or environments without explicit approval from the owner.
Unauthorized Release of Data that is Protected by State or Federal Statute or Regulation	An unauthorized release of data is a communication or physical transfer of confidential information to an unauthorized recipient. Examples include, but are not limited to, a user inadvertently sends a confidential file to an email list, a poorly written application allows users to gain access to sensitive information, and an unencrypted computer or data storage device with confidential information on it is lost or stolen.
Zero-Day Threat	A Zero-Day Threat is a computer threat that exposes undisclosed or unpatched computer vulnerabilities. Zero-day attacks can be considered extremely dangerous because they take advantage of previously unknown vulnerabilities for which no solution is currently available.

1.2 PURPOSE OF THE CYBER INCIDENT RESPONSE PLAN (CIRP)

The CIRP is required in order to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of *[Name of Agency/Department/University/College]* Computer Resources and the Securing of Personal Identifiable Information (PII) and Personal Health Information (PHI). This adverse event may be malicious code attack, unauthorized access to *[Name of Agency/Department/University/College]* systems, unauthorized use of *[Name of Agency/Department/University/College]* services, general misuse of systems and failure to secure PPI and PHI information.

1.3 PURPOSE OF THE INCIDENT RESPONSE TEAM (IRT)

The purpose of *[Name of Agency/Department/University/College]* Incident Response Team is to:

- Protect *[Name of Agency/Department/University/College]* information assets.
- Provide subject matter expertise with managing and handling incidents.
- Determine the extent to which the incident poses problems related to identity theft, loss of individuals', companies' or businesses' privacy or confidentiality or the security of *[Name of Agency/Department/University/College]* information and systems.
- Manage activities to recover from the breach and mitigate the resulting damage, including decisions relating to external breach notification.
- The team will implement the response plan, engage the proper resources and track the efforts and the progress of containing the breach.
- Prevent the use of *[Name of Agency/Department/University/College]* systems in attacks against other systems (which could cause us to incur legal liability).
- Minimize the potential for negative exposure with *[Name of Agency/Department/University/College]* reputation and regaining and building public trust.

1.4 OBJECTIVES OF THE INCIDENT RESPONSE TEAM (IRT)

The objectives of *[Name of Agency/Department/University/College]* Incident Response Team are to:

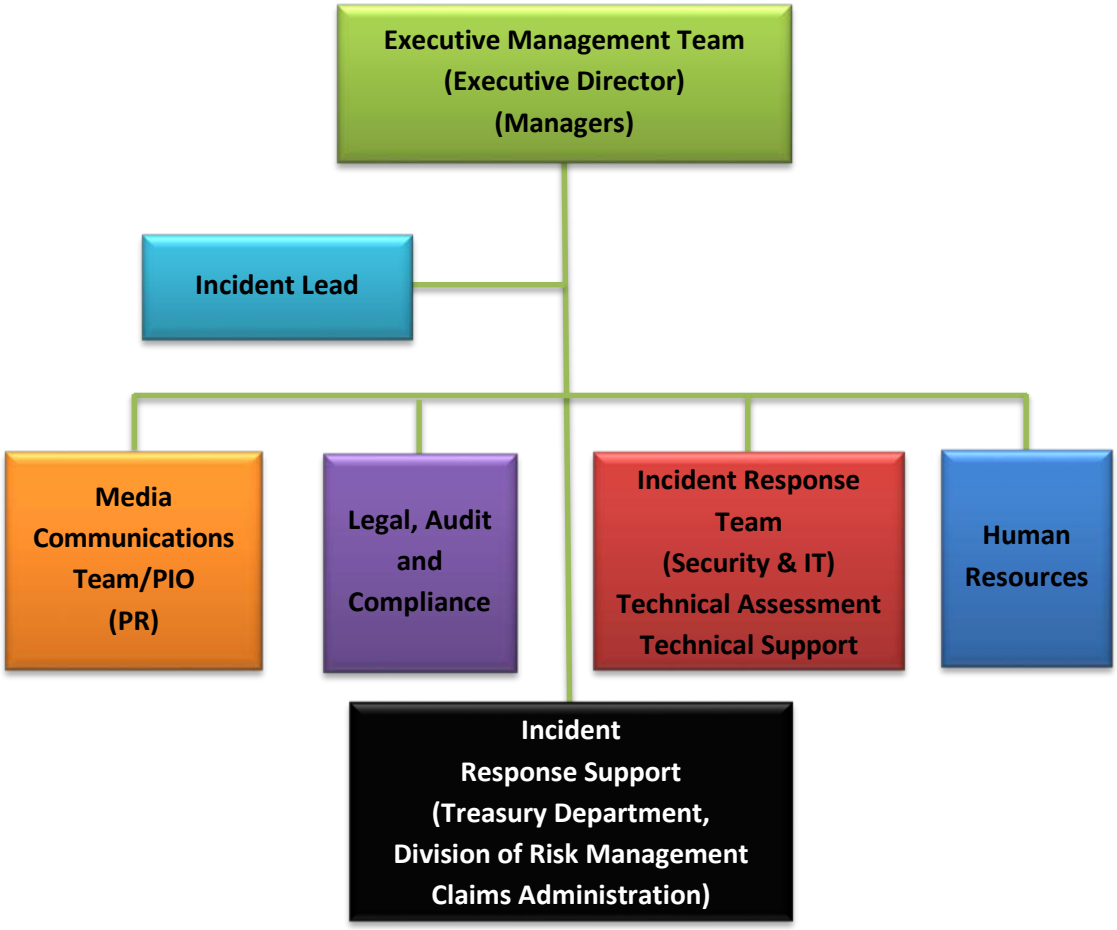
- Contain and minimize threat.
- Determine who initiated the incident. Identify key tasks, manage timelines and document all response efforts from beginning to end.
- Assign and establish team roles and responsibilities, along with specifying access credentials.

- Determine how the incident occurred.
- Avoid escalation and further incidents from specific breach.
- Limit immediate incident impact to customers and partners.
- Summarize the steps needed to assess the scope of a breach.
- Assess the impact and damage in terms of financial harm, reputational harm or other harm.
- Recover from the incident.
- Outline the budget and resources needed to handle a breach.
- Find out how to avoid further exploitation of the same vulnerability.
- Update policies and procedures as needed.
- Ensure contact lists remain updated and team members remain ready to respond.
- Analyze response efforts post-breach to better prepare the *[Name of Agency/Department/University/College]* and team for the next incident.

1.5 INCIDENT RESPONSE TEAM STRUCTURE AND COLOR CODE

To adequately respond to an intrusion or incident, predetermined teams will participate depending on the incident characteristics. As the situation develops and the impact becomes more significant, the various teams will be called to contribute.

See **Appendix A** for list of names and contact numbers for IRT Members.


Executive Management Team
(Executive Director)
(Managers)
Incident Lead
Media
Communications
Team/PIO
(PR)
Legal, Audit
and
Compliance
Incident Response
Team
(Security & IT)
Technical Assessment
Technical Support
Human
Resources
Incident
Response Support
(Treasury Department,
Division of Risk Management
Claims Administration)

2.0 INCIDENTS

2.1 THE FOUR FUNDAMENTAL WAYS DATA BREACHES OCCUR

- Theft or Loss of Physical Equipment - A data breach can occur with the theft or loss of physical equipment which stores data, such as laptop computers or memory storage devices.
- Illegal Access to the Systems or Information - A data breach can occur through malicious code, denial of service, unauthorized access, and unlawful access to PII data by technological means such as hacking into existing computer systems or hijacking computers with viruses, worms or Trojans. Once inside a system, a cyber-criminal can steal data, infect it or overload computer systems.
- Insiders - A data breach can be committed by current employees, ex-employees or even through social engineering where an employee is tricked into providing access or unauthorized release of sensitive information either within or outside of the State such as, but not limited to, phishing, spear phishing, hacking into social networks, and other socially-engineered fraud.
- Oversight - A data breach can occur when no one thought the information needed to be protected and no precautions were taken to safeguard the data in the first place.

2.2 THE SIX STAGES OF RESPONSE

(1) **Preparation** - One of the most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run through the practice of table top exercises and annual training. Review your information system(s) and data and identify where PII, PHI and other sensitive information resides. This can be done by the following:

- Documenting what PII, PHI and other sensitive information is maintained by your organization, where it is stored (including backup storage and archived data), and how it is kept secure;
- Conducting regular risk assessments and evaluating privacy threats for your organization, as well as any contractors, vendors, and other business partners;
- Reviewing who is approved for access to PII, PHI and/or other sensitive information and checking user activity status to determine which accounts should be deactivated after a pre-determined period of inactivity;
- Reviewing separation of duties to help ensure integrity of security checks and balances as employees should only have access to information related to their job function;

- Implementing mitigation controls designed to prevent and detect unauthorized access, theft or misuse of PII, PHI and/or other sensitive data, which includes hard copy files;
- Implementing security controls, such as encryption of sensitive data in motion and at rest (where feasible);
- Regularly reviewing and keeping up-to-date your data destruction policies, to minimize the risk of data breaches through unauthorized access to archived media or computers that are no longer in use; and
- **Annually review and update your CIRP and conduct table top exercises that shall include the Executive Management Team.**

(2) **Incident Discovery/Detection** - It is important that anyone who reports a security incident provides as much relevant information as possible. Based upon the type of the incident, notifications need to go to the appropriate people in the Incident Classification Chart. Additionally, the IRT will identify the appropriate technical teams that are needed to assist with the analysis phase of the incident.

(3) **Triage and Analysis** - Involves limiting the scope and magnitude of an incident because some incidents may involve malicious code and these types of incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment. Also, involves the containment of stolen or unauthorized access to electronic stored data or disseminated of information to an external data base. During this phase of the Incident Handling, it is important to initially identify the criticality of the incident (this may be changed during the analysis phase). This will be done by the IL and IRT. The IL and IRT should consider and determine that an incident may have a State-wide impact. The IL and IRT will undertake appropriate root cause analysis and actions to minimize the risk to state's core business operations.

(4) **Eradication and Recovery** - Restoring a system to its normal business status is essential. Once a restore or recovery has been performed, it is important to verify that the restore operation was successful and that the system is back to its normal condition or the breached data has been contained.

- A computer forensic examination of all loss of data shall be conducted to determine all possible external electronic storage locations.
- This computer forensic examination shall also verify if the breached data has or has not been disseminated to any other known or unknown external electronic location.
- The IL shall document all ongoing events, all people involved and all discoveries into a timeline for evidentiary use.

- The EMT will determine if external notification process shall be activated *(affected individuals, affected businesses, local law enforcement, FBI and/or contracted cyber response vendors)*.
- To determine whether notification of a breach is required, the likely risk of harm caused by the breach and then the level of risk must be assessed.
- A wide range of harm should be considered, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. Removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators or dismissing employees.

(5) **Initial Notification** - Identify whether or not an incident has occurred. If one has occurred, the incident response team (IRT) can take the appropriate actions. If the initial cyber incident is determined to be moderate or high, the EMT shall notify and activate appropriate segments of the Incident Response Team (IRT) and determine if Tennessee Bureau of Investigation involvement is warranted. **Agencies shall report actual or suspected data breaches and suspected data breaches and significant cyber security incidents within 24 hours of discovery to the State Comptroller, the State Treasurer, and the Treasury Department, Division of Risk Management Claims Administration.** Depending on the totality of the circumstances, these guidelines recommend consideration of when an agency or higher learning institution should notify the State Attorney General, the Executive Branch, the Chancellors of the Tennessee Board of Regents, and the University of Tennessee as applicable, and, if determined, members of the General Assembly. **All Departments are still subject to audit by the Comptroller of the Treasury authorized by Tennessee Code Annotated, Section 8-4-109(a)(2).**

- **The highest appointed/elected official (Executive Director) in the EMT shall determine if the [Name of Agency/Department/University/College] will notify the State of Tennessee Board of Regents Chancellor, the University of Tennessee Chancellor, Legislative Branch, Treasurer, Comptroller, Secretary of State, Attorney General, and the Executive Branch.**
- The internal notification process shall include details of the incident, initial risk rating (Low, Moderate, High), as well as the actions that have been taken to respond to the incident thus far.
- Upon discovery, the Incident Lead (IL) of the Incident Response Team (IRT) shall report actual or suspected breaches, significant breaches of departmental data or significant cyber security incidents to *[Name of Agency/Department]* Executive Management Team immediately (EMT) and as soon as possible to the Department of Treasury, Division of Risk Management Claims Administration, if a brief status report of what has occurred is determined by IRT. The IRT will work with the EMT to

record the incident information and the details of the breach in the Cyber Incident Investigation Report Form Note: For individual instances of malware, the IRT should not be activated.

Consider the following:

- ✓ How difficult is it to contain the incident?
- ✓ How fast is the incident spreading?

(6) **Follow-Up** - Performing follow-up activity is one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law.

- This includes, but not limited to, changing *[Name of Agency/Department/University/College]* policies as appropriate. After an incident is resolved, all incidents that have reached a severity of Level 4 or higher will be reviewed by the CSIRT and CISO and a final incident report will be compiled to ensure that all existing processes were followed and were adequate.
- Schedule a lessons-learned meeting with IRT and EMT to discuss any identified improvements to the response plan and the processes to the response that worked well during the incident.
- Determine if other external services, such as law enforcement, insurance company, or cyber vendors, should be considered to assist with future cyber breaches and incidents.
- What is the estimated financial impact to [Name of Agency/Department/University/College]?
- Will this affect [Name of Agency/Department/University/College's] image or public trust negatively?
- Maintain logbook of events and develop an investigation report.
- The investigation report shall include, describe and answer the following:
  - ✓ The description of the data lost, including the amount and its sensitivity or classification level.
  - ✓ For cyber security incidents, the nature of the cyber threat (e.g., Advanced Persistent Threat, Zero Day Threat and data exfiltration).
  - ✓ Nature and number of persons affected (e.g., employees, external customers, students, citizens, vendors).
  - ✓ Likelihood data is accessible and usable from unauthorized personnel or cyber criminals.
  - ✓ Likelihood the data was intentionally targeted.

- ✓ Evidence that the compromised data is actually being used to commit identity theft.
- ✓ Strength and effectiveness of security technologies protecting data.
- ✓ Likelihood the breach may lead to harm and the type of harm. Such harm may include confidentiality or fiduciary responsibility, blackmail, disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty.
- ✓ Ability to mitigate the risk of harm.

2.3 INCIDENT CLASSIFICATION AND NOTIFICATION

An incident will be classified as one of six severity levels. These severity levels are based on the impact to *[Name of Agency/Department/University/College]* and can be expressed in terms of financial impact, impact to services and/or performance of *[Name of Agency/Department/University/College]* mission functions, impact to image or impact to public trust.

All security incidents are classified by the actual and potential impacts on day-to-day activities of the State. This criticality review must occur within all phases and, as the criticality changes, appropriate notifications need to be made. As shown in the chart below, the Incident Response Team (IRT) will be notified for all suspected or confirmed incidents starting with incidents triaged and determined to be "Minor" or above in severity. All incidents determined to be severity level "Low" and above will be escalated by the IRT to the Incident Lead (IL). Incidents determined to be "Moderate" and above will be escalated by the IL to the Executive Management Team (EMT). At the EMT's discretion, notification will be given to *(the State of Tennessee Board of Regents Chancellor, the University of Tennessee Chancellor, Legislative Branch, Treasurer, Comptroller, Secretary of State, Attorney General, and the Executive Branch).*

There may be times when other notifications need to take place, and the Notification Target is only the minimum notification requirement. The (STS, UT, or TBR) Command Center is responsible for maintaining up-to-date contact lists. Please contact them to initiate any required contacts that are not already available. [Strategic Technology Solutions-(615) 741-1001 or (800) 342-3276, option 3; University of Tennessee Office of Information Technology (865) 974-2333; Tennessee Board Regents Chief Information Officer (615) 366-4451].

The Incident Response Team (IRT) shall assess data breaches and incidents involving PII, payment card information, federal tax information, PHI, BII, FERPA, PCI, FTI, or all other data breaches and incidents with support from Treasury Department, Division of Risk Management Claims Administration. The assessment will be based on the details included in the incident report and will assign an initial potential impact level of Low,

Moderate or High. The potential impact levels describe the worst case potential impact on the organization, individual person, employee, or vendor of the breach/cyber incident. The Executive Management Team shall determine, as the incident has more impact (severity level increases), the escalation process will be invoked to involve appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident, with as few resources as possible, to reduce the total impact, and to keep tight control. Below category defines the escalation levels with the associated team involvement.

INCIDENT CLASSIFICATION, ESCALATION LEVELS AND NOTIFICATION		
SEVERITY	**DESCRIPTION**	**NOTIFICATION TARGET**
6 - Very High	Multiple systems inoperable or taken offline preventing the performance of daily duties impacting the servicing of customers, or **confirmed** data breach or system compromise of more than one application, system or area, or involving sensitive application or system data.	• EMT • IL • PIO/Media Communications (PR) • Legal • IRT • HR • IRS (Incident Response support-Treasury)
5- High	Single system inoperable or taken offline, preventing the performance of daily duties impacting the servicing of customers, or **confirmed** data breach or system compromise of a single application, system or area involving non-sensitive application or system data.	• EMT • IL • PIO/Media Communications (PR) • Legal • IRT • HR • IRS (Incident Response support-Treasury)
4 - Moderate	Server(s) is operable with minor damage. Minor damage to facility or business areas which prevents the performance of daily duties which impact the servicing of customers, or **unconfirmed** suspected data or system compromise.	• EMT • IL • PIO/Media Communications (PR) • IRT • IRS (Incident Response support-Treasury)
3 - Low	Server operable with no significant degradation of performance or more than five end user sites affected by the same Minor severity event.	• IL • IRT Primary Contact
2 - Minor	More than five workstations, in a single site, blocked for reimaging.	• IRT Primary Contact

1 - Very Minor	Single workstation blocked for reimage. No data compromise.	• No Notification

2.4 ESCALATION CONSIDERATIONS

Executive Management Team (EMT) will consider several characteristics of the incident before escalating the response to a higher level and prior to the EMT determining the severity of the data breach (Low, Moderate or High). The following considerations should be answered by the EMT:

- How wide spread is the incident?
- What is the impact to *[Name of Agency/Department/University/College's]* operations?
- How difficult is it to contain the incident?
- How fast is the incident spreading?
- What is the estimated financial impact to *[Name of Agency/Department/University/College]*?
- Should law enforcement be notified"
- Will this affect *[Name of Agency/Department/University/College's]* public image negatively?

2.5 INCIDENT RESPONSE TEAM'S ROLES AND RESPONSIBILITIES AT EACH ESCALATION LEVEL

The *[Name of Agency/Department/University/College]* EMT and IRT will determine the appropriate course of action, including notification to affected individuals, the resources needed, and any appropriate remedy options. The EMT and IRT shall notify the State of Tennessee Division of Risk Management Claims Administration (DRMCA) for insurance purposes. The EMT and/or IRT may request additional support from DRMCA upon request.

ESCALATION LEVEL 1 - VERY MINOR	
Normal Operations	• Monitor all known sources for alerts or notification of a threat. Single workstation blocked for reimage. No data compromised. NO NOTIFICATION REQUIRED.

ESCALATION LEVEL 2 - MINOR	
Incident Response Team - Primary Contact	• Verify that an incident has actually occurred. This activity typically involves the unit systems administrator and end user, but may also result from proactive incident detection work of the Security Office or central IT operations. If it is determined that an incident has occurred, inform appropriate authorities. • Monitor all known sources for alerts or notification of a threat. More than five workstation blocked for reimage. No data compromised. • Determine if the Incident Lead needs to be contacted to escalate to Levels 3, 4, 5, or 6.

ESCALATION LEVEL 3 - LOW	
Incident Response Team - Primary Contact	• Conduct a thorough assessment of the type and scope of data exposed following applicable laws, regulation, and policy. • Determine initial defensive action required. • Notify the Incident Lead. • Server operable with no significant degradation of performance, or more than five end user sites affected by the same minor severity event. • Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, and restore operations if the incident compromised or otherwise put out of service a system or network, and ensure that future risk of exposure is mitigated.
Incident Lead	• Based upon the incident classification, determine if an "Executive Communications Team" needs to be formed. • Receive and track all reported potential threats. • Escalate Incident Response to appropriate Escalation Level if a report is received indicating that the threat has manifested itself. • Determine relevant assignment of tasks for personnel to conduct the assessment the data breach has been confirmed. • Alert IT organizatons and applicable support organizations of the potential threat and any defensive action required. • Alert the Executive Management Team and the Communication Team of the potential threat if determined the incident needs to esclate to Levels 4, 5, or 6. • Alert Legal, Audit and Compliance of the potential threat if determined the incident needs to esclate to Levels 5 and 6. • Notify the Incident Response Support Team (DRMCA) of the potential threat if determined the incident needs to esclate to Levels 4, 5, or 6.

ESCALATION LEVEL 4 - MODERATE	
Executive Management Team	• Assume responsibility for directing activities in regard to the incident. • Determine whether Escalation Level 4 is appropriate or escalate to Level 5, or possibly Level 6. • Determine when the risk has been mitigated to an acceptable level. • Executive Director determines when internal notification process should be activated. • Executive Director determines if Tennessee Bureau of Investigation notification process should be activated. • Determine when the breach of data has been either contained or mitigated to an acceptable level through the activation of the computer forensic examination. • Determine if external notification process shall be activated (affected individuals, affected businesses, local law enforcement, FBI and/or contracted cyber response vendors). • Ensure a computer forensic examination of all loss of data will be conducted to determine all possible external electronic storage locations. • Determine risk of harm caused by the breach and then the level of risk must be assessed to esclate to Levels 5 or 6. • **Determine if notice to individuals whose data may have been exposed by the incident is addressed. Swiftness in notifying those affected by a breach of personally identifiable information (PII), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.**

ESCALATION LEVEL 4 - MODERATE	
Incident Lead ***Note:*** *The chronological log will be used to support possible follow up on legal action as determined by [Name of Agency/ Department/ University/College] General Counsel, and Executive Director.*	• **Notify the Executive Management Team of the manefestation of the threat.** • **Notify the Incident Response Support Team (DRMCA) of the incident.** • **Receive status from the Technical Assessment Team and report to the Executive Management Team.** • Start a chronological log of events.
Incident Response Team -Technical Assessment	• **Determine best course of action for containment of the incident.** • **Report actions taken and status to the Incident Lead.** • **Report actions taken and status to the Incident Response Coordinator.**
Incident Response Team - Technical Support	• Take whatever action as determined by the Technical Assessment Team. • Report actions taken, number of personnel involved etc. to Incident Coordinator for the chronological log.
Communication Team/PIO ***Note:*** *The Communication and Executive Management Teams should consider notifying the public media as soon as possible after the discovery of a breach. However, if possible, the incident response plan and notification content should be*	• Message the *[Name of Agency/Department/University/College]* employee population informing them of the incident if deemed appropriate by the Executive Management Team. • Message the *[Name of Agency/Department/University/College]* employee population of any action they need to take as determined by the Technical Assessment Team and directed by the Executive Management Team. • Determine, with Legal, Audit and Compliance, the specific legal obligations and timeline for notification. • Assist the Executive Management Team with determining if or when the data breach should be released to affected individuals and/or the media.

developed prior to notifying the media.	• Notification content should focus on providing information, including links to resources, to aid the public in its response to the breach.
ESCALATION LEVEL 4 - MODERATE	
Communication Team/PIO *(continued)*	• Notification may be delayed upon the request of law enforcement. • To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust.
Incident Reponse Support (Risk Management Claims Administration - Treasury)	• Obtain copy of initial investigation report from the Incident Lead or the Executive Management Team. • Notify State of Tennessee's insurance broker and insurance carrier. • Submit the initial investigation report to insurance carrier and broker. • Determine if a recommendation to activate cyber reponse vendors is needed to the Incident Lead or the Executive Management Team. • Respond to any request for assistance from the Incident Lead or the Executive Management Team.

ESCALATION LEVEL 5 - HIGH	
Executive Management Team	• Direct the Incident Response Support Team to: ✓ Set up communications between all Executive Team Managers and the Techncal Support Team. ✓ Establish and assume occupancy of the command center. ✓ Initialize an incident voice mail box where status messages can be placed to keep *[Name of Agency/Department/University/College]* personnel updated. • Executive Director determines if Tennessee Bureau of Investigation (TBI) notification process should be activated. In some circumstances, the Executive Director, Executive Team Managers, and TBI may consider delaying external notification to affected individuals and media if a notification would seriously impede the investigation of the breach or the affected parties. However, any delay should not worsen risk or harm to any affected individual. • Alert the Extended Team of the incident notifying them of the Severity Level. • Determine when external notification process shall be activated (affected individuals, affected businesses, local law enforcement, FBI, and/or contracted cyber response vendors). • Determine when a computer forensic examination of all loss of data will be conducted to determine all possible external electronic storage locations. • Determine when the risk has been mitigated to an acceptable level. • Provide status updates from Executive Director to the leadership heiarchy within the *[Name of Agency/ Department/ University/College]*. • Ensure that all needed information is being collected to support legal action or financial restitution. • Determine if the information that has been lost or stolen is properly protected by encryption and has been validated by the Technical Assessment Team. If it is determined that the data is encrypted, the risk of compromise may be low to nonexistent.

	• Determine if and when the cyber vendor's call center and monitoring services will be used for the data breach/cyber incident.
ESCALATION LEVEL 5 - HIGH	
Executive Management Team *(continued)*	• **Determine if notice to individuals whose data may have been exposed by the incident is addressed. Swiftness in notifying those affected by a breach of personally identifiable information (PII), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.**
Incident Lead	• Continue maintaining the chronological log of event. • Post numbered status messages in the incident voice mail box for updating agency executive management. • Continue to have oversight over the tasks and progress of the Technical Assessment Team and the Technical Support Team. • Report progress of both the Technical Assessment Team and the Technical Support Team to the Executive Management Team.
Incident Reponse Team - Technical Assessment	• Continue to monitor all known sources for alerts, looking for further information or actions needed to eliminate the threat. • Continue reporting status to the Incident Lead for the chronological log of events. • Monitor effectiveness of actions taken and modify them as necessary. • Provide status updates to the Incident Lead on effectiveness of actions taken and progress in eliminating the threat.
Incident Reponse Team - Technical Support	• Continue actions to eradicate the threat as directed by the Executive Management Team, the Incident Lead, and the Technical Assessment team.

- Continue to report actions taken, number of personnel, etc. to the Incident Lead for the chronological log.

ESCALATION LEVEL 5 - HIGH	
Legal, Audit and Compliance	• Determine, with Communications, the specific legal obligations and timeline for notification. Consult Tennessee Code Annotated, Section 47-18-2107 for specific requirements, and with the Consumer Protection Division of the Attorney General's Office. • Notify the Executive Management Team to determine if or when the data breach notification letter should be released to affected individuals and/or the media. • If the breach involves a state contractor or a public-private vendor operating a system of records on behalf of *[Name of Agency/Department/University/College]*, the Legal, Audit, and Compliance Team is responsible for ensuring or determining if any notification and corrective actions needs to be taken by *[Name of Agency/Department/ University/College]*. • Review contract and outline the roles, responsibilities, and relationships with contractors or vendors, and prepare a summary reflecting cyber insurance requirements within contract. • Work directly with the state-contracted Cyber Coach Attorney and/or obtain an engagment letter with outside counsel or firm that specializes in cyber breaches/ incidents. Consult with Attorney General's Office if an engagement letter is required.
Communication Team/PIO *Note:* *The Communication and Executive Management Teams should consider notifying the public media as soon as possible after the discovery of a breach. However, if possible, the incident response plan and notification content should be*	• Message the *[Name of Agency/Department/University/College]* employee population informing them of the incident if deemed appropriate by the Executive Management Team. • Message the *[Name of Agency/Department/University/College]* employee population of any action they need to take as determined by the Technical Assessment Team and directed by the Executive Management Team. • Determine, with Legal, Audit and Compliance, the specific legal obligations and timeline for notification. • Assist the Executive Management Team with determining if occurrence of the data breach should be released to

developed prior to notifying the media.	affected individuals and/or the media and, if so, when to release information.
ESCALATION LEVEL 5 - HIGH	
Communication Team/PIO *(continued)*	• Notification content should focus on providing information, including links to resources, to aid the public in its response to the breach. • Notification may be delayed upon the request of law enforcement. • To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust.
Incident Reponse Support (Risk Management Claims Administration - Treasury)	• Obtain copy of initial investigation report from the Incident Lead or the Executive Management Team. • Notify State of Tennessee's insurance broker and insurance carrier. • Submit the initial investigation report to insurance carrier and broker. • Determine if a recommendation to activate cyber reponse vendors is needed to the Incident Lead or the Executive Management Team. • Respond to any request for assistance from the Incident Lead or the Executive Management Team.
Human Resources	• HR, Legal, Audit and Compliance, and Executive Director determine disciplinary action or termination is warranted if the breach of data/cyber incident was from an internal source.

ESCALATION LEVEL 6 - Very High	
Executive Management Team	• Direct the Incident Response Support team to: ✓ Set up communications between all Executive Team Managers and the Techncal Support Team. ✓ Establish and assume occupancy of the command center. ✓ Initialize an incident voice mail box where status messages can be placed to keep *[Name of Agency/Department/University/College]* personnel updated. • Executive Director determines if Tennessee Bureau of Investigation (TBI) notification process should be activated. In some circumstances, the Executive Director, Executive Team Managers and TBI may consider delaying external notification to affected individuals and media if a notification would seriously impede the investigation of the breach or the affected parties. However, any delay should not worsen risk or harm to any affected individual. • Alert the Extended Team of the incident notifying them of the Severity Level. • Determine when external notification process shall be activated (affected individuals, affected businesses, local law enforcement, FBI, and/or contracted cyber response vendors). • Determine when a computer forensic examination of all loss of data will be conducted to determine all possible external electronic storage locations. • Determine when the risk has been mitigated to an acceptable level. • Provide status updates from Executive Director to the leadership heiarchy within the *[Name of Agency/ Department/ University/College]*. • Ensure that all needed information is being collected to support legal action or financial restitution. • Determine if the information that has been lost or stolen is properly protected by encryption and has been validated by the Technical Assessment Team. If it is determined that the data is encrypted, the risk of compromise may be low to nonexistent.

	• Determine if and when the cyber vendor's call center and monitoring services will be used for the data breach/cyber incident.
ESCALATION LEVEL 6 - Very High	
Executive Management Team *(continued)*	• **Determine if notice to individuals whose data may have been exposed by the incident is addressed. Swiftness in notifying those affected by a breach of personally identifiable information (PII), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.**
Incident Lead	• Continue maintaining the chronological log of events. • Post numbered status messages in the incident voice mail box for updating agency executive management. • Continue to have oversight over the tasks and progress of the Technical Assessment Team and the Technical Support Team. • Report progress of both the Technical Assessment Team and the Technical Support Team to the Executive Management Team.
Incident Response Team - Technical Assessment	• Continue to monitor all known sources for alerts, looking for further information or actions needed to eliminate the threat. • Continue reporting status to the Incident Lead for the chronological log of events. • Monitor effectiveness of actions taken and modify them as necessary. • Provide status updates to the Incident Lead on effectiveness of actions taken and progress in eliminating the threat.
Incident Reponse Team - Technical Support	• Continue actions to eradicate the threat as directed by the Executive Management Team, the Incident Lead, and the Technical Assessment team.

- Continue to report actions taken, number of personnel, etc. to the Incident Lead for the chronological log.

ESCALATION LEVEL 6 - Very High	
Legal, Audit and Compliance	• Determine, with Communications, the specific legal obligations and timeline for notification. Consult Tennessee Code Annotated, Section 47-18-2107 for specific requirements, and with the Consumer Protection Division of the Attorney General's Office. • Notify the Executive Management Team to determine if or when the data breach notification letter should be released to affected individuals and/or the media. • If the breach involves a state contractor or a public-private vendor operating a system of records on behalf of *[Name of Agency/Department/University/College]*, the Legal, Audit, and Compliance Team is responsible for ensuring or determining if any notification and corrective actions needs to be taken by *[Name of Agency/Department/ University/College]*. • Review contract and outline the roles, responsibilities, and relationships with contractors or vendors, and prepare a summary reflecting cyber insurance requirements within contract. • Work directly with the state-contracted Cyber Coach Attorney and/or obtain an engagment letter with outside counsel or firm that specializes in cyber breaches/ • incidents. Consult with Attorney General's Office if an engagement letter is required.
Comminication Team/PIO *Note:* *The Communication and Executive Management Team should consider notifying the public media as soon as possible after the discovery of a breach. However, if possible, the incident response plan and notification content should be*	• Message the *[Name of Agency/Department/University/College]* employee population informing them of the incident if deemed appropriate by the Executive Management Team. • Message the *[Name of Agency/Department/University/College]* employee population of any action they need to take as determined by the Technical Assessment Team and directed by the Executive Management Team. • Determine, with Legal, Audit and Compliance, the specific legal obligations and timeline for notification. • Assist the Executive Management Team with determining if occurrence of the data breach should be released to

developed prior to notifying the media.	affected individuals and/or the media and, if so, when to release information.
ESCALATION LEVEL 6 - Very High	
Comminication Team/PIO *(continued)*	• Notification content should focus on providing information, including links to resources, to aid the public in its response to the breach. • Notification may be delayed upon the request of law enforcement. • To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust.
Incident Reponse Support (Risk Management Claims Administration)	• Submit updated status reports received from the Incident Lead or the Executive Management Team to insurance carrier. • Determine if a recommendation to activate cyber reponse vendors is needed to the Incident Lead or the Executive Management Team. • Respond to any request for assistance from the Incident Lead or the Executive Management Team. • Assist the Executive Management Team with setting up cyber vendors call center and monitoring services.
Human Resources	• HR, Legal, Audit and Compliance, and Executive Director determine disciplinary action or termination is warranted if the breach of data/cyber incident was from an internal source.

POST INCIDENT	
Incident Lead	Prepare a report for *[Name of Agency/Department/University/College]* executive management to include: • Estimate of damage/impact; • Action taken during the incident (not technical detail); • Follow-up on efforts needed to eliminate or mitigate the vulnerability; • Policies or procedures that require updating; • Efforts taken to minimize liabilities or negative exposure; and • Document lessons learned and modify the Incident Response Plan accordingly.
Legal, Audit and Compliance	• Confirm transmission of any notifications determined necessary by law or policy. • Provide the chronological log and any system audit logs requested by law enforcement or prosecutors, if applicable. • Assist with preparing any or all documents, upon request, from law enforcement or prosecutors, if applicable.
Human Resources	• Determine if any additional training regarding PII, HIPAA, or FERPA is needed for all or certain classes of employees. • Continue with scheduling annual training for PII, HIPAA, or FERPA for all employees.

3.0 CONTENTS OF THE NOTIFICATION

Please note that Legal, Compliance, and Audit divisions should consult Tennessee Code Annotated, Section 47-18-2107 regarding notification requirements.

The notification letter should be provided in writing and should use concise and plain language. The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery.
- A description of the types of personal information involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.).
- A statement regarding whether the information was encrypted or protected by other means when determined such information would be beneficial and would not compromise the security of the system.
- What steps affected parties should take to protect themselves from potential harm, if any.
- What is being done, if anything, to investigate the breach, to mitigate losses and to protect against any further breaches? The inclusion of any details concerning the investigation of the breach should take into consideration whether or not the inclusion of such details would jeopardize an ongoing law enforcement investigation.
- Who should affected parties contact for more information? Include a toll-free call center telephone number, e-mail address, and postal address.
- Given the amount of information required above, the component may want to consider layering the information, providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format, or on the *[Name of Agency/Department/University/College]* website. If the *[Name of Agency/Department/University/College]* has knowledge that the affected parties are not English speaking, notice should also be provided in the appropriate language(s).

See Appendix B for sample of written notifications.

APPENDIX A

CONTACT LISTS

INCIDENT RESPONSE TEAMS:

Executive Management		
Organization	**Contact Name**	**Phone Numbers**

Incident Lead		
Organization	**Contact Name**	**Phone Numbers**

Technical Assessment		
Organization	**Contact Name**	**Phone Numbers**

Technical Support		
Organization	**Contact Name**	**Phone Numbers**

Incident Response Support Team (Division of Risk Management Claims Administration)		
Organization	**Contact Name**	**Phone Numbers**
Treasury Department, Risk Management	Rodney Escobar	615-741-9957(O)
Treasury Department, Risk Management	Jamie Fohl	615-741-9972 (O)

Communications		
Organization	**Contact Name**	**Phone Numbers**
TBR Communications	Richard Locker	615-366-4417

Legal, Audit and Compliance		
Organization	**Contact Name**	**Phone Numbers**
TBR Legal	Mary Moody	615-366-4438
TBR Audit Executive	Tammy Gourley-Birchett	615-366-4407

Human Resources		
Organization	**Contact Name**	**Phone Numbers**
TBR Human Resources	April Preston	615-366-4404

External Notfication List		
Organization	**Contact Name**	**Phone Numbers**
[Name of Cyber Vendor Name] NAS	Jean Cofield	202-429-6557
[Name of Forensic Computer Firm] NAS	Jean Cofield	202-429-6557
[redacted]	Jean Cofield	202-429-6557
[Name of Insurance Carrier] AON	Jean Cofield	202-429-6557

Law Enforcement Notification Contact List		
Organization	**Contact Name**	**Phone Numbers**
Tennessee Bureau of Investigation		615-744-4000
Nashville FBI Office		901-747-4300
Memphis FBI Office		901-747-4300
Knoxville FBI Office		865-544-0751
Chattanooga FBI Office		865-544-0751

SAMPLE WRITTEN NOTIFICATION

DATA ACQUIRED: Social Security Number (SSN)
(Note: Do not insert actual SSN)

Dear:

We are writing to you because of a recent security incident at *[Name of Agency/Department/University/College]*. [Describe what happened in general terms, what kind of PII was involved, and what you are doing in response.]

The *[Name of Agency/Department/University/College]* takes the security of personal information very seriously, and we continue to work closely with the appropriate authorities to continue to monitor this situation. In addition, the *[Name of Agency/Department/University/College]* has taken immediate steps to strengthen its internal controls, and established safeguards to prevent a similar breach.

*[Name of Agency/Department/University/College] i*s notifying you, with this letter, so that you can take actions, along with efforts, to minimize potential harm. *[Name of Agency/Department/University/College]* has also advised the three (3) major credit reporting agencies, in the United States, about this incident and have given those agencies a report, alerting them of this incident.

Even though the *[Name of Agency/Department/University/College]* is not aware that any of the personal information has been used for identity theft or other criminal activity, the *[Name of Agency/Department/University/College]* has taken the added precaution of hiring the identify theft prevention firm *[Name of Vendor]* to provide you with one (1) year of identity protection services, and the optional credit monitoring services, all free of charge.

However, *[Name of Agency/Department/University/College]* also encourages you to protect yourself from the possibility of identity theft. We recommend that you complete a Federal Trade Commission ID Threat Affidavit. This added step will assist you with legally notifying your creditors that your identity may have been compromised. Any debts or newly opened lines of credit incurred, after that date, will not be assigned to you.

We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the numbers below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289

[Name of Agency/Department/University/College] believes you should closely monitor your credit report and place a fraud alert on your credit file. If you do find suspicious activity on your credit report or have reason to believe your information is being misused, please call your local law enforcement agency for assistance. You may also file a complaint with the Federal Trade Commission by visiting www.ftc.gov/bcp/edu/microsites/idtheft or calling 1-877-ID-THEFT (438-4338).

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the Identity Theft website of the Federal Trade Commission.

In closing, *[Name of Agency/Department/University/College]* also encourage you to access the following resources and review the enclosed brochure about identity theft from [Name of Vendor]:

- Federal Trade Commission's website provides information about the three (3) major credit reporting agencies and identity theft consumer alerts: www.ftc.gov/bcp/conline/pubs/alerts/infocompalrt.htm
- Identity Theft Resource Center: www.idtheftcenter.org
- Privacy Rights Clearinghouse: www.privacyrights.org

One of the top priorities of the *[Name of Agency/Department/University/College]* is protecting the personal information that flows through our various programs that we are responsible for administering.

Sincerely,

[Name and Title]

GENERAL GUIDANCE FOR THE ESTABLISHMENT OF A CALL CENTER IN THE EVENT OF A SIGNIFICANT DATA BREACH

In the event of a significant data breach involving PII, the following guidance is provided to help with the determination of whether to establish a call center. The purpose of a call center is to provide individuals a number to call to obtain further information regarding the data loss and possible action they may want to take to lessen the incident's impact on their personal lives.

The decision to establish a call center should be based on several considerations:

- If the breach affects a large number of individuals and those individuals are not easily identifiable or easily contacted, establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the breach.
- Each situation will be unique and the decision to establish a call center must be based on individual circumstances. The main concern should be sharing of information with those affected and how they may obtain assistance.

Once a decision is made to establish a call center, there are several options:

- Contract with external cyber vendor to obtain call center and monitoring services.
- Establish an internal, fully-supported and staffed call center. A thorough description of the incident and set of frequently asked questions (FAQs) will also be required for call center to refer to when fielding calls.

Suggested items to consider based on the nature of the breach would include, but are not limited to, the following:

- Using existing *[Name of Agency/Department/University/College]* personnel to staff the call center and monitoring services, if external cyber vendor services are not used.
- Ensuring training of call center operators.
- Pre-stage FAQs.
- Ability to adjust staffing in response to call volume.
- Daily hours of operations.
- Cost of service.
- Call logging.

- Establish reporting requirements such as dropped calls or wait time, number of callers, etc.
- Advertising call center numbers and making data breach information readily available to those affected.
- Quality assurance checks of call center effectiveness.

SAMPLE CALL CENTER FAQ

EXAMPLE QUESTION	EXAMPLE ANSWER (In case there is no evidence of illegal use of information.)
How can I tell if my information was compromised?	• At this point, there is no evidence that any missing data has been used illegally. However, the *[Name of Agency/Department/University/College]* is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.
What is the earliest date at which suspicious activity might have occurred due to this data breach?	• The information was stolen from an employee of the *[Name of Agency/Department/University/College]* during the month of _____. It is likely that individuals may notice suspicious activity during the month of _____.
I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself from being victimized by credit card fraud or identity theft?	• *[Name of Agency/Department/University/College]* strongly recommends that individuals closely monitor their financial statements, and visit the *[Name of Agency/Department/ University/ College's]* special website at **www._____@tn.gov** for updates regarding this incident.
Should I reach out to my financial institutions or will the *[Name of Agency/ Department/ University/College]* do this for me?	• The *[Name of Agency/Department/University/College]* does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts unless you detect suspicious activity. If so, you will need to report it.

EXAMPLE QUESTION	EXAMPLE ANSWER (In case there is no evidence of illegal use of information.)
Where should I report suspicious or unusual activity?	The Federal Trade Commission (FTC) Identity Theft website (**http://www.consumer.ftc.gov/features/feature-0014-identity-theft**) recommends the following steps if you detect suspicious activity: Immediate Steps: • Place an Initial Fraud Alert. • Contact the fraud department of one of the three major credit bureaus: ✓ Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241 ✓ Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013 ✓ TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790 • Order your credit report from the three major credit bureaus above. • Create an Identity Theft Report. • Submit a report about the theft to the FTC online or call the FTC at 1-877-438-4338 (1-866-653-4261 – TTY). When you finish writing all the details, print a copy of the report. It will be called an Identity Theft Affidavit. Bring your FTC Identity Theft Affidavit when you file a police report. • File a police report with your local police department or the police department where the theft occurred, and get a copy of the police report or the report number. Your FTC Identity Theft Affidavit and your police report make an Identity Theft Report.

EXAMPLE QUESTION	EXAMPLE ANSWER (In case there is no evidence of illegal use of information.)
Where should I report suspicious or unusual activity? *(continued)*	• Consider whether you need an Extended Fraud Alert. If you have created an Identity Theft Report, you can get an extended fraud alert on your credit file. When you place an extended alert, you can get two free credit reports within 12 months from each of the three nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for five years, unless you ask them to put your name back on the list. The extended alert lasts for seven years. • Consider whether you need a Credit Freeze. You may choose to put a credit freeze on your file, but a credit freeze may not stop misuse of your existing accounts or some other types of identity theft. Also, companies that you do business with would still have access to your credit report for some purposes. A fraud alert will allow some creditors to get your report as long as they verify your identity. This measure is only recommended if you have confirmed your identity has been stolen. • Close any accounts that have been tampered with or opened fraudulently.

EXAMPLE QUESTION	EXAMPLE ANSWER (In case there is no evidence of illegal use of information.)
Where can I get further, up-to-date information?	• The *[Name of Agency/Department/University/College]* has set up a special website which features up-to-date news and information. Please visit **www._____@tn.gov**.
Does the data breach affect only certain individual?	• It potentially affects a large population of individuals. We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.
What is the *[Name of Agency/ Department/ University/ College]* doing to ensure that this does not happen again?	• The *[Name of Agency/Department/University/College]* is working with the law enforcement to investigate the data breach and to develop safeguard against similar incidents. The *[Name of Agency/Department/University/College]* has directed all employees to complete the Computer Security Awareness and Training (CSAT)" course. Appropriate law enforcement agencies*, (Name of Law Enforcement Agency/or Department)* have launched full-scale investigations into this matter.
What additional information will I receive regarding this incident?	• You will receive a Notification Letter from *[Name of Agency/Department/University/College]* mailed to you by the *[Name of Agency/Department/University/College]* vendor, *[Name of Cyber Vendor]* ID on ____, (DATE). This letter will include a toll-free telephone number to the *[Name of Cyber Vendor]* call center for any questions and information regarding consumer identity protection, credit monitoring, and identity theft insurance services being provided free through *[Name of Vendor]*. You will be automatically enrolled in the consumer identity protection services. In addition, free optional credit monitoring services with three national credit bureaus and identity theft insurance is also available to those who register for these services. The *[Name of Agency/Department/University/College]* encourages you to take advantage of these free services.

Has the problem been contained?	• *[Name of Agency/Department/University/College]* believes this is an isolated incident and it does not appear that the file has been disseminated to other people or sources.

APPENDIX E

SAMPLE QUESTIONS AND CHECKLIST FOR INVESTIGATION REPORTS

The investigation report shall include, describe, and answer the following:

- The description of the data lost, including the amount and its sensitivity or classification level.
- For cyber security incidents, the nature of the cyber threat (e.g., Advanced Persistent Threat, Zero Day Threat and data exfiltration).
- Nature and number of persons affected (e.g., employees, external customers, students, citizens, vendors).
- Likelihood data is accessible and usable from unauthorized personnel or cyber criminals.
- Likelihood the data was intentionally targeted.
- Evidence that the compromised data is actually being used to commit identity theft.
- Strength and effectiveness of security technologies protecting data.
- Likelihood the breach may lead to harm and the type of harm. Such harm may include confidentiality or fiduciary responsibility, blackmail, disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty.
- Ability to mitigate the risk of harm.
- How wide spread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident spreading?

ATTACHMENT B

RESIDENCY PROPOSAL

For TBR Community Colleges

Overview

The Community College Admissions and Records Directors are proposing common guidance for determining in-state residency classification based upon interpretation of State law. This guidance would be used when a student is initially classified as out-of-state for tuition purposes and then appeals his or her residency decision. The TBR Student Policy is 3:05:01:00.

Purpose

- To establish a common and consistent interpretation across colleges of the policy and the documentation that can be used to classify a student as in-state.
- Establish a baseline for acceptable documentation to prove that Tennessee is student's true and fixed permanent home.
- Establish a common community college framework for consistent decision-making, while still allowing the colleges flexibility in documentation used for in-state residency classification when a student has a unique circumstance.

Rules

- State law says that every person having his or her domicile in Tennessee shall be classified as in-state for fee and tuition purposes.
- Domicile if further defined as "a person's true, fixed, and permanent home and place of habitation; it is the place where he or she intends to remain, and to which he or she expects to return when he or she leaves without intending to establish a new domicile elsewhere."

PROPOSAL:

GUIDANCE FOR RESIDENCY CLASSIFICATION OF STUDENTS

Eligibility to Establish Domicile

Can Establish Domicile

- US Citizens
- Permanent Residents (valid/unexpired)
- Asylees/Refugees
- Visa Types
    - A1 – A3
    - E1, E2
    - G1 – G5
    - H1B, H4
    - I
    - K1 – K4
    - L1, L1a, L1b, L2
    - NATO 1 – NATO 7
    - O1, O3 (dependents of O1 only)
    - P1 – P4
    - R1, R2
    - T1 – T4
    - V

Cannot Establish Domicile

- Students who have not met EVEA
- Undocumented persons
- Persons on Deferred Action (DACA/Dream Act)
- Visa Types
    - B1, B2
    - C1 – C3
    - D1
    - F1, F2
    - H1C, H2A, H2B, H3
    - J1, J2
    - M1, M2
    - N
    - O2, O3 (dependents of O2)
    - Q1 – Q3
    - S5 – S7
    - TC, TN, TD

- U1 – U5

Documentation to Prove Domicile

- Students who are not emancipated must submit parent's, legal guardian's, or foster parent's documentation in lieu of their own.
  - Federal tax returns showing the student is a dependent will be required.
  - A birth certificate for the student may be required if parents are divorced and the student resides with the out-of-state parent.
  - If parents are divorced, a copy of the divorce decree and/or other documentation may be required if the student resides with the out-of-state parent.
  - If a parent who is a TN resident is deceased, a death certificate may be required if the student resides with the out-of-state parent.
- Students who are married may provide their spouse's documentation but must also include a marriage license.
- To prove domicile, students must provide at least one item from Group A, or two items from Group B, or one item from Group B and two items from Group C.

  Group A

  - Proof of receiving a State benefit (i.e. TennCare, Disability, SNAP)
  - Current mortgage or deed for property in TN where the person resides
  - Proof of current classification as in-state for fee purposes at another TN higher education institution (excluding Academic Common Market)
  - Military orders assigning person to TN

  Group B

  - Proof of full-time employment in TN
  - Proof of multiple part-time employment positions equivalent to full-time employment (35 or more hours)
  - A current lease for a residence in TN where the person resides
    - Those not on lease must have a notarized letter from leaseholder regarding their residence arrangement
  - A Federal tax return showing a TN residence from the most recent prior tax year
  - Current enrollment of a Pre-K through 12th grade dependent in a TN public or private school

  Group C

  - Notarized letter from a parent or legal guardian stating the student will not be claimed as a dependent for the current or upcoming Federal Income Tax year
  - Valid non-temporary TN driver's license or State ID
  - Valid TN vehicle registration
  - Valid TN voter's registration
  - DD214 showing TN as the home of record
- Other documentation may be considered at in the individual institution's discretion provided it complies with TBR Policy 3:05:01:00.

Out-of-state Paying In-state Fees

Parent Relocated

Residency Code: P
Policy Section: 2.A

Documentation

- Prior classification as in-state
- Change of permanent address to out of state
- Proof of dependency by one of the following:
    - Federal tax returns showing the student is a dependent
    - A birth certificate for the student listing parent

Military Dependent

Residency Code: Q
Policy Subsection: 2.B

Documentation

- Military orders assigning parent to Ft. Campbell
- Proof of dependency by one of the following:
    - Federal tax returns showing the student is a dependent
    - A birth certificate for the student listing parent

30 Mile Radius

Residency Code: M
Policy Section: 2.C/2.E

Counties

Institution	State	County	Code
APSU	Kentucky	Christian	21047
APSU	Kentucky	Logan	21141
APSU	Kentucky	Todd	21219
APSU	Kentucky	Trigg	21221
ChSCC	Alabama	Jackson	01071
ChSCC	Georgia	Catoosa	13047
ChSCC	Georgia	Dade	13083
ChSCC	Georgia	Murray	13213
ChSCC	Georgia	Walker	13295
ChSCC	Georgia	Whitfield	13313
ClSCC	Georgia	Walker	13295
ClSCC	Georgia	Whitfield	13313
ClSCC	Georgia	Murray	13213
ClSCC	Georgia	Fannin	13111
ClSCC	Georgia	Catoosa	13047
DSCC	Arkansas	Mississippi	05093
DSCC	Missouri	Dunkin	29069

Institution	State	County	Code
DSCC	Missouri	Pemiscot	29155
MSCC	Alabama	Madison	01089
MSCC	Alabama	Jackson	01071
NaSCC	Kentucky	Christian	21047
NaSCC	Kentucky	Logan	21141
NaSCC	Kentucky	Todd	21219
NaSCC	Kentucky	Trigg	21221
NeSCC	Virginia	Washington	51191
NeSCC	Virginia	Bristol City	51520
NeSCC	Virginia	Scott	51169
NeSCC	North Carolina	Mitchell	37121
NeSCC	North Carolina	Watauga	37189
STCC	Arkansas	Mississippi	05093
STCC	Arkansas	Crittenden	05035
STCC	Mississippi	Desoto	28033
STCC	Mississippi	Marshall	28093
VSCC	Kentucky	Allen	21003
VSCC	Kentucky	Logan	21141
VSCC	Kentucky	Simpson	21213
WSCC	Virginia	Lee	51105
WSCC	North Carolina	Haywood	37087
WSCC	North Carolina	Madison	37115
WSCC	North Carolina	Mitchell	37121
WSCC	North Carolina	Swain	37173
WSCC	North Carolina	Yancey	37199
WSCC	Kentucky	Bell	21013
WSCC	Kentucky	Whitley	21235

Documentation (Required for Reclassification)

- Current mortgage or deed for property within the 30 mile radius where the person resides or a current lease for a residence within the 30 mile radius where the person resides
    - Those not on lease must have a notarized letter from leaseholder regarding their residence arrangement

Border County

Residency Code: J
Policy Section: 2.D/2.E.1/2.E.2

Counties

Institution	State	County	Code
APSU	Kentucky	Allen	21003
APSU	Kentucky	Calloway	21035
APSU	Kentucky	Simpson	21213
ETSU	North Carolina	Ashe	37009
ETSU	North Carolina	Avery	37011
ETSU	North Carolina	Haywood	37087
ETSU	North Carolina	Madison	37115
ETSU	North Carolina	Mitchell	37121
ETSU	North Carolina	Watauga	37189
ETSU	North Carolina	Yancey	37199
ETSU	Virginia	Grayson	51077
ETSU	Virginia	Lee	51105
ETSU	Virginia	Scott	51169
ETSU	Virginia	Washington	51191
ETSU	Virginia	Bristol City	51520
TTU	Kentucky	Clinton	21053
TTU	Kentucky	Cumberland	21057
TTU	Kentucky	McCreary	21147
TTU	Kentucky	Monroe	21171
TTU	Kentucky	Wayne	21231
TTU	Kentucky	Whitley	21235
UM*	Arkansas	Crittenden	05035
UM*	Mississippi	Desoto	28033
UM*	Mississippi	Marshall	28093
UM*	Mississippi	Tate	28137
UM	Mississippi	Tunica	28143
ChSCC	Georgia	Fannin	13111
MSCC	Alabama	Limestone	01083
NaSCC	Kentucky	Allen	21003
NaSCC	Kentucky	Calloway	21035
NaSCC	Kentucky	Simpson	21213
VSCC	Kentucky	Clinton	21053
VSCC	Kentucky	Cumberland	21057
VSCC	Kentucky	Monroe	21171

*Changing to 30 Mile Radius July 1, 2016

Documentation (Required for Reclassification)

- Current mortgage or deed for property in the border county where the person resides or a current lease for a residence in the border county where the person resides
    - Those not on lease must have a notarized letter from leaseholder regarding their residence arrangement

FT Employee, PT Student (Work Rule)

Residency Code: A
Policy Subsection: 2.F

Documentation

- Proof of full-time employment in TN or proof of multiple part-time employment positions equivalent to full-time employment (35 or more hours)
- Current mortgage or deed for property not in TN where the person resides or a current lease for a residence not in TN where the person resides
    - Those not on lease must have a notarized letter from leaseholder regarding their residence arrangement

Veteran

Residency Code: 9
Policy Section: 2.L

Documentation

- Proof of discharge with an honorable characterization of service
- Proof of eligibility for Post-9/11 GI Bill benefits or Montgomery GI Bill benefits
- Enrollment at a TBR institution within three years of from the date of discharge as reflected on the veteran's DD214 or equivalent document.

Residency Reclassification

Reclassification to In-state

Student was not initially able to establish domicile in TN and was paying out-of-state fees. A significant change must have occurred for the student to be reclassified. Examples would be, but are not limited to:

- Marriage to a person who is eligible for in-state classification
- Purchase a home in TN with the intent of residing there
- Obtain full time employment in TN
- Parent of an unemancipated student establishes domicile in TN
- Permanent residency/citizenship is obtained
- Relocate to a border county or location classified as within the 30 mile radius

Reclassification to Out-of-state

If the institution becomes aware of a change in the student's domicile, reclassification to out-of-state status may occur. A break in enrollment may also result in reclassification if the student's domicile changes.

Adjusted Fee Rate (eRate)

TBR Guideline B-060.IV

Requirement

Be classified as a non-resident of Tennessee and be enrolled exclusively in online courses

Attachment C

Proposed Language for Study Abroad Business Procedures

Budgeting

Each study abroad program is expected to be financially self-sustaining over time, and be accountable for good financial management practices. A projected budget must be completed by the Study Abroad Program Director and submitted to the sponsoring institution's Chief Business Officer or his/her designee.

The budgeting process for study abroad programs should be based on a reasonable projection of operating costs in the host country, including consideration of projected currency exchange rates. The budget should also clearly identify which expenses are to be paid from tuition and mandatory course fees and which expenses are to be paid from the student-specific program fee revenue. The budget should also specify if the expense is for the employee or students.

Budgeting for instructional costs paid from the general fund may consider both tuition revenues and state appropriations generated by student enrollments in study abroad programs, consistent with budgeting for other academic programs.

In addition, the budgeting process should include the establishment of a reserve fund, appropriate to the size and scale of the institution's programs, to ensure that the institution can meet reasonable contingencies that may arise during the operation of the program. It is recommended that an amount not less than 5% or more than 20% of the program fees be budgeted for this reserve.

Registration and Fee Payment

Students who participate in approved study abroad programs should normally be assessed tuition and program fees by their home institution (or the sponsoring institution) Business Office. Study Abroad Offices and program directors should avoid the direct receipt of payments from students, whenever possible. Study Abroad Offices and program directors should provide the Business Office necessary information about each student and his/her appropriate program charges, so that these can be entered into the institution's student information system.

Study abroad fees generally consist of two components:

1. **Tuition and mandatory student fees related to the actual registration for classes.** All study abroad students pay a minimum of tuition and applicable mandatory fees. Whenever possible, tuition should be assessed by the regular student information system when registration occurs. Payment due dates and refund dates should be the same as those for students taking campus-based courses.

2. **Program specific fees (for travel, lodging, meals, exchange rate variance, etc.**) These program fees should be assessed in the student information system whenever possible. The payment deadlines and refund schedules for these fees will vary from program to program. Payment due dates and refund dates can be earlier, but should not be later, than the due dates and refund dates for students taking campus-based courses.

Accounting

Financial activity attributable to study abroad programs in recorded in two funds: General funds (Unrestricted E&G) and Agency funds.

1. Student tuition and applicable mandatory fee revenue is assessed and recorded in General funds (E&G) as tuition revenue. Salaries and benefits of program faculty and staff should be paid from applicable departmental E&G funds.

   Note: Costs of instruction and other instructionally related costs such as employee travel, lodging, meals, as well as other instructional expenses such as tutors, lecturers, room rental, etc., may be paid from E&G funds.

2. Program Fee revenue and related expenses are recorded in an Agency Fund account specific to the responsible program or office. Student-specific expenses must be paid from the Agency account. Typical student-specific costs include travel, lodging, tours, meals, event fees, and student supplies. Students are also assessed an additional program fee to cover such things as the cost of travel and non-instructional costs of conducting the program. The Program Director may also elect to charge a per-person amount for emergency funds.

   Note: If an agency account has been inactive for eighteen months, with no deposits or expenditures, any excess funds remaining in the account must be transferred to another study abroad program fund or to the general fund.

Both the activity's self-supporting and agency funds should be monitored and regularly reconciled by the Study Abroad Office. It should also be verified that only activity-related expenses are charged to self-supporting funds. The institution may choose to refund residual balances in the self-supporting fund among activity participants, or use this money to establish and maintain a contingency account. However, any unused personal funds remaining in the related agency fund at the end of the program must be refunded to the participants who submitted the funds.

Acquiring Goods and Services Abroad

To the maximum extent possible, arrangements for goods and services needed while abroad should be paid directly to the vendor from the General fund account and/or Agency account established for the study abroad program. However, there are situations where payment for goods and services abroad must be rendered at the time they are acquired. In these situations institutions may utilize several methods to make payments while abroad.

Any of the following can be used for purchases and expenses associated with a study abroad program:

- Procurement card
- Bank account in foreign country
- Check request
- Stored value/pre-paid card
- Traveler's check
- Cash Advance/petty cash advance to an authorized institutional representative
- Direct payment by an authorized institutional representative from personal funds, with a reimbursement request to follow

Study abroad programs should comply with all applicable TBR and institution policies regarding procurement and use of these payment methods.

Petty Cash - Each institution will have the authority to determine the best way to handle payment of purchases and expenses for its study abroad programs. A petty cash fund may be established to pay for goods/services while in a foreign country. However, due to the risks and responsibilities associated with petty cash, its use should be limited to those situations where other payment alternatives are not an option.

Institutions using petty cash should have the following in place:

- Petty cash application and approval process
- Procedures for opening a petty cash bank account
- Reconciliation guidelines
- Closeout guidelines
- Management, record-keeping, and reimbursement procedure

Travel Advance - Institutions may also allow for travel advances to pay for large expenses abroad. All travel advances should follow current institution policies. The employee must include the estimated foreign expenses that will be required to be paid in cash, along with an explanation of why they cannot be paid for with a credit card or direct billing arrangement. The employee must provide information to clearly show the business purpose of the expenses and documentation to support the expenses claimed.

Upon return, the employee must complete a travel expense voucher and submit itemized receipts for all expenses paid from the advance. If the expenses were less than the amount of advance received, all remaining funds must be returned to the institution. If costs were more than what was provided in the

travel advance for expenses that are approved or integrally related to the educational aspects of the program, the employee may receive reimbursement for these expenses.

Reimbursement

Employees are responsible for keeping copies of original receipts to verify that expenses were valid and related to the program. If it isn't possible to obtain original receipts for program-related expenses, the employee must keep a log listing all expenses and ask the person providing the service to sign and document what was provided. The institution will hold the employee financially responsible for all charges for which there are no receipts or log entries. The employee will also be responsible for all expenses that are not approved according to TBR or institution regulations, as well as those not integrally related to the educational aspects of the program.

Whether the employee owes money back to the institution or is eligible for reimbursement, he/she is responsible for completing the Travel Expense Report and submitting it with all appropriate receipts within 30 following their return to the United States. Reimbursements that are not submitted within a reasonable amount of time are considered taxable by the IRS and must be processed through the payroll system.

The following items must be completed and submitted to the Study Abroad Office no later than 10 days after the conclusion of the study abroad trip:

1. List of program participants with student ID numbers and amount of program fees paid by each participant.
2. List of faculty, including course names and numbers, section numbers, credit hours for classes taught, and names of students in each class.
3. All bank statements, if applicable to the program.
4. Documentation of foreign exchange rates used. This will only apply if funds were exchanged during the program. (www.oanda.com is a good resource for currency conversion.) If currency is bought in advance, please provide documentation of the rate at which the currency was originally purchased.
5. Required documentation of expenses – including receipts for goods and services purchased, and signature sheets for cash allowances distributed during the program.
6. Do not include disallowed expenses on the Travel Expense Summary and Travel Expense Report. Examples of disallowed expenses include personal items, alcohol, etc.
7. The Travel Expense Summary and a summary of travel advances should be submitted with the Travel Expense Report.
8. The Travel Expense Report must be filled out in U.S. dollars and signed by the Study Abroad Program Director or his/her designee.
9. Upon return from the trip, remaining institution funds must be deposited in the Business Office with a deposit receipt form. A copy of the deposit receipt form must be submitted to the Study Abroad Office if funds were deposited.

10. If foreign currency was distributed to the program director in advance of the trip, documentation must be submitted with the Travel Expense Report. This also applies if foreign currency was returned to the Study Abroad/Business Office.

Attachment D

Formatted: Right

Procurement Card Guideline: B-125

Guideline Area

General Guidelines

Applicable Divisions

TCATs, Community Colleges, Universities, System Office

Purpose

The purpose of this procurement card guideline is to provide parameters in the areas of program administration, file management, proper procurement card usage, and to promote compliance with Tennessee Board of Regents (TBR) Policies and Guidelines. This Guideline is subject to regular update, revision and improvement.

Definitions

Approver – means the institution's employee who approves PCard transactions.

Cardholder – means the Institution's employee who is issued a physical PCard to initiate purchases/payments on behalf of the Institution.

Cardholder Agreement – means the document signed by the Cardholder to verify that he or she has completed PCard training, received a copy of the PCard Policy, PCard Guideline, and training manual and understands his or her responsibilities.

Commercial Card Provider – means the financial institution that provides the PCards and related services.

Institution – means any of the universities, community colleges, colleges of applied technology and System Office departments within the Tennessee Board of Regents.

Merchant Category Codes (MCCs) – the codes assigned by an acquiring financial institution, that identifies the primary goods or services a vendor provides.

Monthly Credit Limits – means the spending limit that restricts the total value of purchases a Cardholder can make in one billing cycle.

PCard Program – means the program established by the Institution and managed by the PCard Program Administrator whereby Cardholders make purchases on behalf of the Institution.

PCard Program Administrator – means the employee within the institution who is responsible for managing and overseeing the PCard Program.

Procurement Card or PCard - means a corporate liability credit card issued by the Institution's contracted commercial card provider that allows institutions to make purchases/electronic payments for goods or services. A PCard is similar to a consumer credit card, but the card-using institution must pay the card issuer in full each month. In this Policy, the term "Procurement Card" or "PCard" shall also include "Virtual/Ghost Procurement Cards" or "Virtual/Ghost PCards" as the context requires.

Purchase Transaction Limit – means the mandatory spending limit that restricts the amount of a single purchase regardless of the monthly credit limit on the card.

Reconciler – means the Institution's employee responsible for all functions associated with post-purchase processing PCard transactions, including matching expenses to the financial institution's cardholder statement and verification of account allocation.

System Office – the administrative offices of the Tennessee Board of Regents.

Virtual/Ghost Procurement Cards – means a unique account number which is assigned to a department for payment of vendors with an existing relationship with the Institution.

Guideline

I. Introduction.

The PCard Program is a program developed to streamline the purchasing process, including procurement, receiving, and payment processing. This Guideline governs an Institution's PCard Program in conjunction with all applicable state, TBR, and Institution Policies and Guidelines. Cardholders must use discretion and be good stewards when making purchases and/or incurring expenses on behalf of the Institution.

II. PROGRAM ADMINISTRATION

A. PCard Services/Management

The PCard program is administered by each Institution. Responsibilities include the application process, issuing and canceling cards, initial training, and managing the daily operations of the program.

B. Program Procedures/Compliance

Each Institution shall designate individuals to direct program compliance by utilizing various review methods. These methods may include annual compliance reviews, transaction reviews, introductory reviews for new cardholders, and other reviews as deemed appropriate and necessary.

Other areas of responsibility may include training, distribution of educational materials, initial set up of general ledger accounts, set up of user account credentials for the Institution's PCard software, and any amendments to Institutional procedures necessary to comply with TBR and Institution policies.

C. Audit Services

The Institution’s auditing personnel shall assist in auditing the purchasing card program, and may decide to conduct an official audit of an individual PCard and/or an Institution's PCard program.

III. PROCUREMENT CARD PROGRAM/OPERATING PROCEDURES

A. PCard Application Process

The Institution PCard program is reserved for eligible personnel as determined by the Institution. To obtain a PCard, an employee must satisfy all steps of the Institution’s process before a card will be issued.

B. Program Requirements

To remain eligible for participation in the PCard program, Institution cardholders, approvers, and support staff must adhere to the following requirements:

1. Application Process

   Institutions shall have a defined process in which eligible personnel apply/complete a request to obtain a PCard. (See Exhibit 1 for sample) There will be no credit reference check on the personal credit of the employee for the PCard, nor will the use of the PCard have any impact on the employee's personal credit rating. The account number for the PCard Program is a credit card number issued in the name of the employee, who is responsible for ensuring that all purchases made using the card are for official Institution purchases. Legitimate charges to the PCard are an Institution Liability (not a personal liability to the individual cardholder).

2. Training

   Cardholders, and others identified by the Institution, are required to receive training prior to the activation of a PCard and the date of training must be documented. Upon completion of training, the employee shall sign a Cardholder Agreement. (See Exhibit 2 for sample) The Institution shall maintain a training manual that includes procedures and administrative resources for the Cardholder.

3. Terminating Employment

   In the event of termination, the cardholder must return the PCard to the Institution or destroy the card at the direction of the program administrator. A review will be conducted by the Institution's designee prior to the employee's departure or final compensation.

4. Departmental Transfer

   When a cardholder transfers to another position within the Institution, the cardholder shall work with the Institution's PCard Program Administrator to take appropriate action.

5. Leave of Absence

   When a leave of absence has been granted, the Institution's PCard Program Administrator may suspend cardholder's PCard during the leave of absence.

6. Voluntary Termination or Card Suspension

   When a cardholder voluntarily terminates its Pcard account or it is deemed necessary by the Institution to suspend card privileges, the Institution shall maintain adequate documentation to support the change in cardholder status. (See Exhibit 3 for sample)

C. Disputing Fraudulent Charge(s)

It is mandatory that the cardholder immediately notify the Institution's PCard Program Administrator, the commercial card provider, and any designated Institution personnel when fraudulent activity is suspected or verified. The cardholder will work with the Institution to complete the required documentation from the commercial card provider. (See Exhibit 4 for a sample)

D. Lost or Stolen PCard

Cardholders must report a lost or stolen card to the commercial card provider and Institution's PCard Program Administrator as soon as possible. The cardholder's reporting efforts must be documented for audit purposes.

E. File Management Requirements

Maintaining complete PCard file documentation is a requirement of the program. The Institution will only be responsible for business purchases supported by original receipts, invoices, and/or supporting documentation directly from a vendor. Cardholders and approvers could be held personally liable for undocumented or unauthorized purchases. PCard privileges may be revoked for file mismanagement.

1. All purchases, including online vendors, must have an itemized receipt identifying the goods or services purchased. Receipts are the primary method used by the Institution's PCard Program Administrator to support business related purchases. Packaging slips, invoices, or other equivalent documentation should be maintained for all purchases when available.

2. If a receipt is misplaced, the cardholder must contact the vendor to request a copy of the receipt. If the vendor cannot replace the receipt, the cardholder must complete the required Institution's PCard Program documentation. (See Exhibit 5 for a sample).

3. Documentation, such as required policy approval forms, policy exception memos, and other related institution required documentation must be kept on file with the original purchase receipt.

4. Monthly activity logs detailing the transactions may be maintained (See Exhibit 6 for sample). The monthly commercial card statements, original receipts, invoices, and other supporting documentation shall be included as backup for each log. This information must be retained in accordance with the Records Retention and Disposal of Records Guideline (G-070).

5. Cardholders and/or support staff are responsible for reviewing and resolving all back orders, unfilled orders, sales tax charges, credits refunded by vendors, and fraudulent charges.

6. Cardholders and approvers are responsible for assigning purchases to the correct ERP account codes.

7. Card purchases must be shipped to an Institution location, department or to Institution's Central Receiving.

8. Approvers are required to check receipts and monthly reconciliations on a routine basis per the Institution's PCard Program requirements and address any issues or fraudulent charges if discovered.

F. PCard Usage Parameters

Purchase Transaction Limits shall be established according to the Institution's policies and procedures. Monthly Credit Limits are set by Institution's PCard Program Administrator.

Merchant Category Codes (MCC) – the Institution shall make a determination with the commercial card provider regarding any MCC Code restrictions.

G. Sales Tax

It is the cardholder's responsibility to ensure the Institution is not charged sales and/or use tax when purchasing goods and services. Upon request, a sales tax exemption certificate shall be provided to the vendor. Reasonable measures must be pursued by the cardholder to recover taxes paid on the PCard and efforts are to be documented.

H. Unallowable PCard Practices

1. Splitting Purchases

The practice of splitting purchases of goods or services for the purpose of evading State purchasing requirements is a direct violation of TBR purchasing policies, and may result in revocation of PCard privileges (TBR Purchasing Guideline B-120, Section V.3.). Splitting purchases includes, but is not limited to:

a. Splitting a purchase with one vendor into multiple orders.

b. Using two (2) or more cards for purchases from the same vendor.

c. Multiple purchases with the same vendor over the span of a few days.

Cardholders that purchase or anticipate purchasing more than established bid limit amounts during a fiscal year with a non-contracted vendor shall contact Institution's Procurement Office for possible bidding/contract options.

2. Departmental PCards

PCards that are issued in the name of the department, in lieu of an individual, shall have an assigned custodian for the card. The custodian shall maintain documentation related to departmental employees that check in/out the card and the details all purchases, with receipt/backup documentation maintained. .

3. Purchasing Goods and Services with Non-Contracted Vendors

Institution's should utilize State of Tennessee, TBR (including all TBR Institutions and TBR approved Group Purchasing Organizations (GPO)) and University of Tennessee contracts as primary sources for purchases.

If the good or service desired can be procured at a lower price or is unavailable on current contracts, the Institution may purchase with another vendor. All PCard purchases shall be made with due diligence and fiscal responsibility.

J. Prohibited Transactions

The following items are excluded from the Pcard Program and may not be obtained with a Pcard:

a. Personal purchases and cash withdrawals
b. Gift Cards
c. Travel expenses, with the exception of conference registration fees, airline tickets, required advance hotel payments, and team/group travel expenses incurred during actual travel time
d. Equipment (as defined under TBR Guideline B-110, Fixed Assets and Sensitive Minor Equipment)
e. Any other category as mandated by the Institution

K. Non-Compliance and Consequences

1. Violations and Reimbursements

Under certain circumstances, cardholders and/or approvers may be required to reimburse the Institution for unallowable purchases.

PCard privileges may be suspended until the Institution has been reimbursed.

Situations that may require reimbursement include but are not limited to the following:

a. Charges incurred outside of applicable TBR/Institution policies.

b. The inability to document purchases with receipts and/or other supporting documentation.

c. The continued purchase of unallowable goods and/or services where the cardholder has received previous notice(s) of non-compliance from Institution's PCard Program Administrator.

d. Any occurrence where Institution and/or grant funds are subject to substantial waste and/or abuse by the cardholder and/or approver.

The Cardholder will be required to reimburse the Institution for any personal purchases placed on the PCard. In some instances, non-compliance could result in the permanent revocation of PCard privileges, personal reimbursement, and/or termination of employment.

2. PCard Mismanagement

Cardholder and/or Approver mismanagement of PCard privileges when procuring goods and services outside the parameters of this policy or other policies may result in adverse action. Consequences will depend on the severity of the violations identified.

3. Consequences for Non-Compliance

a. Temporary Suspension

PCard privileges may be temporarily suspended for any cardholder and/or department who does not comply with all policies and regulations pertaining to the use of PCards. The decision to suspend privileges and the duration of suspensions will be determined based upon the severity of the violation(s), the number of offenses, and the department's ability to take corrective action.

b. Other Corrective Action

Intentional use of a PCard for any purposes other than state business will result in disciplinary action, up to and including termination from state employment or criminal prosecution.

L. Reporting Fraud, Fiscal Misconduct, or Violation of TBR Financial Policies

Institution employees who know or suspect that other employees are engaged in theft, fraud, embezzlement, fiscal misconduct or violation of Institution or TBR policies and guidelines have a responsibility to report its concerns in accordance with State Law.

Exhibits –

Exhibit 1 – PCard Request Form

Exhibit 2 – Cardholder Agreement Form

Exhibit 3 – Change in Cardholder Status Form

Exhibit 4 – Disputed Charge/Items Form

Exhibit 5 – Lost Receipt Form

Exhibit 6 – Pcard Activity Log Form

Exhibit 1

PCARD REQUEST FORM

To be signed by the appropriate Approvers responsible for the budgetary account.
Complete one form for each cardholder.

Cardholder Name (please print): _____
Employee Number: _____ Email: _____
Department Name: _____
Name of PCard Reconciler: _____
Cardholder's Campus Box Number: _____
Cardholder's Business Phone: _____
Cardholder is (check one): _____Permanent Employee _____ Temporary Employee

I am authorizing the above named employee to receive a [Institution] PCard for the department of

_____for the account number listed below.

_____ _____
Approved by (Director, Dept. Chairperson, Principal Investigator) Date

_____ _____
Approved by (Dean/Administrative Officer) Date

Use of the card is restricted to purchases in accordance with the terms and conditions outlined in the PCard Guidelines.

Default Index Code and Account Code: _____ / _____

Requested Monthly Credit Limit - Circle one:

$1,000 $1,500 $2,000 $5,000 $8,000 $10,000 Other amount: _____

(If an amount is not indicated, the account will automatically be set at $2,000.)

Please add here any special requests or comments, such as "Group Travel" or "Need to use at Restaurants:" _____

Return completed and signed form to the PCard Program Administrator

Exhibit 2

EMPLOYEE CARDHOLDER AGREEMENT
FOR [INSTITUTION] PCARD

You have been approved to receive a PCard for your Institution. Please complete the following.

DATE: _____

NAME: _____
Print Name as it will appear on the PCard

The employee/representative is to complete this agreement after completing the appropriate training and after reading the appropriate PCard policies and guidelines.

You are hereby authorized to make purchases and pay for such purchases using the [Institution] PCard as provided in [Institution]'s policies and guidelines.

Purchases may be made consistent with your organizational responsibilities, including any grant restrictions, to conduct legitimate [Institution] business. All purchases must be made in accordance with applicable Institution and/or TBR policies and procedures and are subject to PCard monetary limits as established by the appropriate approving authority and/or provisions of [Institution]'s policies and guidelines.

Cardholder's PCard account(s) shall terminate upon separation of employment/agency from [Institution] or upon reassignment to another department within [Institution].

(Cardholder please initial each statement.) I understand that:

_____ I am responsible for the safeguarding and security of my PCard;
_____ Any charges incurred, including sales tax, which are expressly prohibited by any policy/procedures of [Institution], will be my personal responsibility;
_____The PCard is not to be used for personal purchases, and any such charge shall be reimbursed by me;
_____ [Institution] has the right to cancel my PCard at any time;
_____In the event I use the card in a fraudulent manner, the Institution may take appropriate disciplinary action, up to and including termination of my employment.

****

_____
Cardholder's Signature

_____
Department

_____ _____
Date Training Completed Signature of PCard Trainer

Change in Cardholder Status Form

Office of Business and Finance – Policy IV: 04:22

CARDHOLDER INFORMATION			
Cardholder Name:			**Today's Date:**
Current Department:		**Current Approver:**	

CHANGE IN CARDHOLDER STATUS			
☐ **Cardholder Termination**	**Effective Date:**	**Last Paid Date:**	**Reason for Termination:** ☐ Resignation ☐ Retirement ☐ Dismissal ☐ Change in Benefited Status
☐ **Departmental Transfer**	**Effective Date:**	**Activation Date in New Position:**	**Departmental Index:**
	Department:	**Position:**	**Approver's Name:**
☐ **Leave of Absence**	**Effective Date:**	**Expected Date of Return:**	**Comments:**
☐ **Discontinued Use of P-Card**	**Effective Date:**	**Reason for discontinuing the use of the P-Card:**	

CHANGE IN STATUS CHECKLIST (Required per Policy IV:04:22)		
Does the approver have the cardholder's files in their possession?	☐ Yes	No
If the cardholder is **TERMINATING** employment or **DISCONTINUING** the use of their P-Card, has the P-Card been returned to Procurement Services?	Yes	No
Have the cardholder's receipts been reconciled to purchases in ESP?	☐ Yes	☐ No
Have the cardholder's purchases been coded to the correct Banner account code?	Yes	No
Have all of the cardholder's purchases been approved in ESP?	☐ Yes	☐ No
Are there any outstanding purchases not recorded in ESP?	Yes	No

As the approver, I am certifying all of the information above is accurate and all processes have been completed.

Name of Cardholder	**Cardholder's Signature**	**Date**
Name of Approver	**Approver's Signature**	**Date**
Name of New Approver (If Departmental Transfer)	**Approver's signature**	**Date**

Copy: Office of Business and Finance (CAB 106) **Original Copy: Cardholder's File** **Copy: New Approver (If Departmental Transfer)**

Disputed Charges Form

Keep a copy for your records before sending the dispute form.

Name	
Account Number	
Transaction Date	Posting Date
Institution Name	Dollar Amount

Signature (Required)	Date
Best Contact Number	Home Telephone
Business Telephone	Cell Telephone

Choose only one dispute reason.

☐ The amount of the charge was increased from $_____ to $_____ or my sales slip was added incorrectly. Enclosed is a copy of the sales slip that shows the correct amount.

☐ I have not received the merchandise that was to be shipped to me by the expected delivery date of __/__/__, (MM/DD/YY). I have asked the merchant to credit my account.

☐ I was issued a credit slip that has not shown on my statement. A copy of the credit slip is enclosed. The merchant has up to 30 days to credit the account.

☐ Merchandise that was shipped to me has arrived damaged and/or defective. I returned it on __/__/__ (MM/DD/YY) and asked the merchant to credit my account. Enclosed is a letter describing how the merchandise was damaged and/or defective and a copy of my return receipt. (REQUIRED)

☐ Although I did engage in the above transaction, I have contacted the merchant, returned the merchandise on __/__/__ (MM/DD/YY) and requested a credit. I either did not receive this credit or it was unsatisfactory. Attach a letter explaining why you are disputing this charge with a copy of proof of return. Also, if you are unable to return the merchandise, please explain.

☐ The services that were to be provided on __/__/__ (MM/DD/YY) were not received or were unsatisfactory. I contacted the merchant by phone or e-mail on __/__/__ (MM/DD/YY) for credit. Attach a letter describing the services you expected, the merchant's response to your attempts to resolve the dispute and enclose a copy of your sales contract/agreement.

☐ I certify that the charge in question was a single transaction, but was billed _____ times for the same charge by this merchant. I did not authorize _____ transactions. Enclosed is a copy of my sales slip.

Sale Number 1	Reference Number 1
Sale Number 2	Reference Number 2

☐ I received the merchandise or services; however, the merchant was paid by another method, (cash, check(s), or another credit card)
(PROOF OF PAYMENT REQUIRED)

☐ I notified the merchant on __/__/__ (MM/DD/YY) to cancel the pre-authorized order. I am requesting a credit. Please send copy of cancellation letter or note person spoke with at time of cancellation. Give reason for cancellation _____ and cancellation number _____.

☐ I notified the merchant and cancelled the hotel, motel or lodging reservation(s) on __/__/__ (MM/DD/YY). The cancellation number or code is _____.

☐ Cash received by ATM was less than requested. Amount requested$_____. Amount received $_____. Please provide copy of ATM receipt

☐ I certify that I do not recognize the transaction. Merchants often provide telephone numbers next to their name on your billing statement. Please attempt to contact the merchant for information.

☒ I certify that the charge listed above was not made by me or a person authorized by me to use my card, nor were the goods or services represented by the transaction received by me or a person authorized by me.

☐ My credit card was (circle one) Stolen, Lost, Never Received, Never Out of My Possession, But Still Misused on or about __/__/__.

☐ If your dispute is for a different reason, please contact us at the above telephone number. For prompt service, please have the account number available for the charge in question.

☐ If needed, please add another sheet for additional comments and/or disputed charges.

☐ I am no longer disputing this previously disputed transaction.

Purchasing Card
Lost Receipt/Invoice Affidavit
Office of Business and Finance

Cardholder Name			
Approver Name			
Department		**Last 4 Digits of Card**	

I certify that I made the purchase shown below for official business but do not have a receipt. Ihave documented my requests for an itemized receipt from the vendor in my P-Card files.

Reason for form (Check all that apply):

- ☐ Vendor did not provide a detailed receipt.
- ☐ I have requested an invoice, but the vendor cannot provided it.
- ☐ I had a receipt but cannot locate it.
- ☐ I have a receipt but it is not readable or the descriptions are notunderstandable.

All information must be typed. All information is required. Use one affidavit for each lost receipt. All affidavits over **$50.00** must be approved by the Dean or Vice-President.

Vendor Name	
Date of purchase	

Detailed Description of Items Purchased	Item Amount
Total Purchase Amount	

This document will be used in lieu of an invoice or receipt for this transaction. I certify that all items listed above were purchased for business use for the Institution and received on its behalf.

I also understand that multiple missing receipts over a period of time will result in suspension or termination of purchasing card privileges.

Cardholder Signature: _____ Date: _____

Approver Signature: _____ Date: _____

Dean/VP Name (Print): _____

Dean/VP Signature: _____ Date: _____

Exhibit 6

PCARD ACTIVITY LOG

Name:_____

Department:_____

PCard #_____(last 4 digits)

Reconciled By: _____ Date: _____

Approved By: _____ Date: _____

Order Date	Vendor/Contact/ Phone #	Quantity/Description	Charges (or Refunds)	Index & Account Code	Date Merchandise Received	Reconciled With Statement

The Activity Log is designed as a tool that can be used to keep track of items purchased and the dollar amount spent using the PCard. The Activity Log entries presented below are representative of the information that should be recorded. Another form of documentation with comparable information is acceptable. If departments are comfortable with comparing supporting documentation to the [Commercial Card Provider] statements, that is an acceptable procedure. Each department can determine specific uses for the activity log to better control their PCard activity. The only requirements are noted below.

An activity log, or other supporting documentation, is required when orders/credits are made via the telephone or any other method and a receipt is not immediately available. These orders shall be documented to ensure accuracy of items received and amounts charged. This will also provide documentation of all credits due the University since credits often occur after a time lag.

Visa account statements and supporting documentation have the same retention requirements as other accounts payable records. These transaction records must be kept in the department and may only be destroyed in accordance with procedures as detailed in TBR Guideline G-070.

Shown below is a sample activity log:

Order Date	**Vendor/Contact/ Phone #**	**Quantity/Description**	**Charges (or Refunds)**	**Index & Account Code**	**Date Merchandise Received**	**Reconciled With Statement**
8/11/14	Staples	3 Staplers, returned	($21.00)	262001 74510	8/13/14	√
8/12/14	Walmart/Pickup	Film Processing	$9.50	262001 74510	8/14/14	√
8/13/14	PC Computing	Computer Supplies	$45.00	262001 74510	8/15/14	√

Status of IT Audit Recommendations

as of 7/26/2016

School	Original Report Date	Date next documentation due	Number of Recommendations Reported	Corrective Action Completed	Still open
APSU	4/22/2015	**7/1/2016**	16	10	6
ETSU	N/A	N/A	N/A	N/A	N/A
MTSU	9/8/2015	8/15/2016	15	11	4
TSU	5/11/2015	9/1/2016	19	13	6
TTU	9/10/2015	9/1/2016	14	8	6
UOM	N/A	N/A	N/A	N/A	N/A
ChSCC	4/12/2016	10/3/2016	20	0	20
ClSCC	4/6/2015	9/1/2016	17	12	5
CoSCC	7/24/2015	**7/1/2016**	16	11	5
DSCC	8/14/2015	9/1/2016	15	5	10
JSCC	9/8/2014	12/30/2016	11	9	**2**
MSCC	4/15/2016	10/14/2016	17	0	17
NaSCC	Report not yet released		13	0	13
NESCC	Report not yet released		18	0	18
PSCC	9/3/2014	12/30/2016	20	19	**1**
RSCC	4/17/2015	12/30/2016	15	13	**2**
STCC	7/6/2015	9/30/2016	17	6	11
VSCC	5/13/2016	11/30/2016	15	0	15
WSCC	3/2/2016	9/30/2016	15	0	15
TBR Sys Office	5/23/2014	**7/1/2016**	16	13	3
Research & Assessment	5/11/2015	**completed**	3	3	0
TN e-Campus	3/2/2016	10/7/2016	16	0	16
TCATs	Report not yet released		TBD	0	TBD

308	133	175
100%	43%	57%
37%	Initial date not	115
19%	Date extensior	60

Attachment L

Formatted: Right

Guideline Area

General Guidelines

Applicable Divisions

TCATs, Community Colleges, Universities, System Office, Board Members

Purpose

The purpose of this policy is to establish minimum standards of expectations related to maintaining appropriate software versions and upgrades within the institutional infrastructure.

Guideline

I. Policy

A. Enterprise information systems and components used at Tennessee Board of Regents' institutions should maintain appropriate and timely updates/patches/maintenance to ensure that systems, data, and personal identifiable information (PII) are adequately protected.

B. Maintaining proper oversight and implementation of this policy will help to:

1. Reduce system vulnerability,
2. Provide consistent system-wide support,
3. Ensure compatibility with other systems, and
4. Enhance application functionality.

C. It is important that institutional executive and oversight leadership support the necessary functions and processes required in order to ensure that systems and data are protected and secure.

II. Scope

A. This policy applies to all enterprise information systems, software, and components.

1. This would include, but not be limited to web systems, end-user applications, infrastructure and end-user information systems, and all other software and hardware not specifically noted.

B. Enterprise Information Systems Update Priorities

1. The following are the priorities and timeframes within which updates must be applied:
    a. Develop institutional approval and sign-off procedures based on the update requirements.
    b. Schedule to not be subject to change except in the most extreme circumstances.
    c. Be communicated to students, faculty and staff in a timely manner.
    d. Critical updates/fixes should be applied as soon as is possible in accordance with institutional approval and sign-off procedures.

C. Enterprise Information Systems Covered By This Policy

1. ERP Quarterly Updates should be installed in in their entirety and in a timely manner. The institution should not be more than one version behind the current ERP vendor-certified release.
2. Oracle CPU Updates should be installed in a timely manner and the institution should not be more than one version behind the ERP vendor-certified ~~current~~ release.
3. External application and system hosting will conform to institutional requirements with written exceptions being made as necessary based on the abilities and contractual obligations between the institution and the hosting vendor.
4. Operating System (OS) updates for servers, workstations, and other end user equipment should be installed in a timely manner in accordance to institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.
5. End-user applications regular and critical updates should be installed in a timely manner in accordance to institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.
6. Network infrastructure and systems regular and critical updates should be installed in a timely manner in accordance with institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.

7. All other enterprise information systems and components regular and critical updates should be installed in a timely manner in accordance to institutional needs and requirements, and to minimize and avoid unduly exposing the institution to risks.

III. Exceptions

A. Exceptions to items 1. and 2. under Enterprise Information Systems Covered by this policy must be approved by the President/CEO at the institution and filed with the Chancellor and System CIO.

B. Other exceptions to this policy may be approved by the CIO or most senior information technology (IT) official at the institution.

C. Each exception must be documented in detail and retained for future review.

Sources

New Guideline approved at Presidents Meeting, August 19, 2014, effective September 26, 2014.

Related Policies

- Information Technology Resources

Contact

Mickey Sheen
615-366-4437
mickey.sheen@tbr.edu