TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

No. 1104 **Rev.: 2**

Policies and Procedures **Date: March 29, 2018**

Subject: Privacy

1. Purpose

This policy sets forth Tidewater Community College's position regarding the protection of individual privacy and the confidentiality of personally identifiable information provided by its employees, students, and visitors, whether that information is provided in an electronic or physical form.

The Government Data Collection and Dissemination Practices Act (*Code of Virginia* § 2.2-3800 *et seq*.) requires that "Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse." This provision does not distinguish between information maintained in electronic or physical form—i.e., digital/computer-stored or paper records. Other state and federal laws and regulations govern specific types of personal information.

2. Policy

Tidewater Community College is committed to protecting individual privacy and to ensuring the confidentiality of personally identifiable information provided by its employees, students, and visitors. To that end, TCC has developed and promulgated the Information Privacy Statement appearing in Appendix A. This statement shall be published on the college's website and in its student and employee handbooks. A companion Web Privacy Statement shall be published on the college's website.

2.1. Personal Information

For agencies and institutions of the Commonwealth, "Personal Information" (PI) is defined in the *Code of Virginia* § 2.2-3801 (see the definition on page 14). As a practical matter, TCC considers PI to be any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

1. Names and Numbers:
    a. Name (when combined with other elements of PI listed below)
    b. Date and year of birth
    c. Social Security number
    d. Mother's maiden name

e. Official state-issued or US-issued driver's license or identification number
f. Alien registration number
g. Government passport number
h. Employer or taxpayer identification number
i. Medicaid or food stamp account number
j. Bank account number
k. Credit or debit card number
l. Personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;

2. Unique biometric data, such as fingerprint, voiceprint, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code;
4. Medical records;
5. Academic grades;
6. Telecommunication identifying information or access device;
7. Other number or information that can be used to access a person's financial resources.

It is TCC's policy and practice to collect the least amount of PI necessary to fulfill its required duties and responsibilities, to complete a particular transaction, to deliver services, or as required by law. This applies to the collection of all PI regardless of source or medium.

Information shall be shared only with college employees or students of TCC who have a need to know in order to provide services or conduct college business. TCC may share PI with other individuals or organizations that provide services to the college only as necessary to provide the services. TCC requires these third parties to protect PI it receives pursuant to this policy and applicable law. The college will take reasonable and appropriate measures to protect PI from unauthorized access or disclosure.

As a public institution, some PI maintained by TCC may be subject to disclosure pursuant to The Virginia Freedom of Information Act (*Code of Virginia* § 2.2-3700 *et seq.*). In addition, TCC may disclose information to third parties when such disclosure is required or permitted by law.

Additionally, as stipulated in the *Code of Virginia* § 2.2-3801, "…routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject" is not considered PI. For example, an office phone tree used for contacting staff in the event of an emergency~~,~~ would not be considered PI under the law or this policy.

2.2. Compliance with Relevant Laws

TCC will comply with the relevant provisions of the various state and federal statutes governing privacy in the workplace and for students, to the extent that they apply to the college's operations, including but not limited to:

1. Government Data Collection and Dissemination Practices Act (*Code of Virginia* § 2.2-3800 *et seq*.)
2. The Virginia Freedom of Information Act (*Code of Virginia* § 2.2-3700 *et seq.*)
3. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
4. Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 *et seq*.).
5. Fair and Accurate Credit Transactions Act (FACT Act) (16 C.F.R. Part 681.
6. Financial Services Modernization Act (Gramm-Leach-Bliley Act) (15 U.S.C. § 6801 *et seq*.)
7. Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)

2.3. College Privacy Officer

The College Privacy Officer shall be appointed by the College President to oversee all TCC activities related to the development, implementation, maintenance of, and adherence to the college's policies and procedures covering the privacy of, and access to, personal information in compliance with federal and state laws. The College Privacy Officer shall have the responsibilities delineated in Appendix B. In the event the College Privacy Officer is not available the College's Information Security Officer (ISO) will be the backup individual for the Privacy Officer.

2.4. Privacy Oversight Committee

The members of the Privacy Oversight Committee shall be appointed by the College President to assist the College Privacy Officer in evaluating and recommending a corrective action and recovery plan, including any plans for mitigation, where appropriate as per the college's policies and procedures covering the privacy of, and access to, personal information. The committee will include representation from the President's Executive Staff, in addition to departments and individuals who can lend a college-wide perspective to privacy implementation and compliance. The College Privacy Officer will serve as chair of the Privacy Oversight Committee.

2.5. Investigating and Responding to Privacy Violations

Tidewater Community College will investigate and attempt to resolve all complaints and confirmed incidents relating to breaches of privacy and confidentiality within a reasonable time after a complaint is received or a privacy incident is reported.

No member of the college community will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or reporting a privacy incident, or inquiring about how to file a complaint or incident report.

Appropriate sanctions will be applied against college employees or students who fail to comply with the college's privacy and security policies and procedures or with federal and state privacy and security regulations.

The College Privacy Officer will serve as the college's central contact and investigation authority for privacy complaints, incidents, and breaches, including coordinating privacy notifications when required. To that end, the College Privacy Officer will:

1. establish and administer a process for receiving, documenting, tracking, investigating, and taking action on complaints concerning TCC's privacy policies and procedures;
2. review and determine action on privacy complaints and incident reports filed with the college;
3. ensure consistent application of sanctions for failure to comply with privacy policies by members of the college community;
4. document all privacy complaints and reported privacy incidents, including:
    a. the findings from reviewing each complaint and incident;
    b. a description of corrective actions taken, or an explanation of why corrective actions are not needed;
    c. a description of risk assessments completed;
    d. any notification procedures taken, including recommendations and final approvals; and
    e. any mitigation undertaken for each specific complaint or incident.
5. retain documentation for all privacy complaints and incidents for at least six years, or longer if required by law or other circumstances.

TCC will make reasonable efforts to notify affected persons if it is determined that their personal information was, or is reasonably believed to have been, acquired by an unauthorized person and that the information could be used for fraudulent purposes. Notification to affected individuals will include the following components:

1. a general description of the incident;
2. the police report number, if available;
3. the type of information subject to the unauthorized access or disclosure
4. instructions and necessary information for notifying the major credit agencies of suspected or potential identity theft;
5. the College Privacy Officer's contact information, including telephone number, e-mail address, and postal mailing address.

6. advice to remain vigilant by reviewing account statements and monitoring free credit reports; and
7. other information as deemed necessary

If appropriate based on the scope of the violation, the notification will also be posted on the TCC website.

3. Responsibilities

The College Privacy Officer shall develop and promulgate procedures to implement the policy delineated above.

4. Procedures

The following procedures implement TCC's Privacy Policy. They apply to all college records, including computer-based and paper, that contain Personal Information (PI).

Tidewater Community College is committed to protecting the Personal Information of its students, employees, alumni, and any others whose PI it collects and stores. In the event of a compromise of PI, the college will take appropriate action to notify all individuals whose information was subject to the compromise. Individuals are subject to sanctions for the failure to comply with security measures or any intentional misconduct that results in a compromise of PI.

4.1. Protecting Personal Information

Various state and federal laws and regulations govern the collection and safeguarding of Personal Information (PI) and require those who collect PI to follow strict guidelines. Protecting such sensitive information is especially important because of the potentially severe consequences of identity theft for the individual whose PI is compromised.

All college departments should follow good practices in safeguarding all PI. Every TCC employee or student who has access to PI—either intentional or inadvertent—must work to help the college meet the requirements imposed by the relevant laws and regulations that govern the protection of PI. To that end, Appendix C, "Guidelines for Protecting PI," will be made available on the college's website and in those work areas in which PI is routinely collected, stored, or used in college business practices.

PI will not be collected, stored, or used except as required by law, or needed to perform core college business activities that cannot be immediately facilitated by other means. The respective college vice president/administrator shall determine whether such collection, storage, or use is required to conduct the college's business as follows:

- Executive Vice President for Academic and Student Affairs – student and alumni records (including the centrally managed Student Information System, other than its financial modules)
- Associate Vice President for Human Resources – personnel records

- Vice President for Finance – financial records (including those containing PI in the Administrative Information System and in the financial modules of the Student Information System)
- Vice President for Information Systems – infrastructure systems (e.g., the college e-mail system and the voice-mail system)

To the extent feasible, PI will be collected, stored, and processed only via centrally managed systems (e.g., the Student Information System). The following measures shall be followed to protect PI from compromise.

1. No college employee will download PI from a centrally managed information system or otherwise create a data file—including an ad hoc report or query from a centrally managed system such as the Student Information System—that contains PI without specific authorization from the appropriate administrator as identified above—Appendix D provides a process to review requests to establish such local data files, including the concurrence of the College Information Security Officer.
2. PI will not be stored on college-owned local computing systems except as specifically authorized by the college vice president/administrator as delineated above. (PI will not be stored on a personally-owned computing system.) When PI is authorized for local storage and processing, the data file(s) will be stored in a designated directory on a network server that is backed up routinely.
3. Except as required to provide information to other government agencies or authorized third-party partners in support of college business, data files containing PI will not be transferred to computing systems that are not under the college's control. Data files containing PI will not be transferred or downloaded to an employee's personal computing system.
4. Data files containing PI will not be stored on any portable computing system (e.g., laptop computer, etc.), whether college-owned or not.
5. Data files containing PI may be transferred or downloaded to portable storage media (e.g., disk, CD/DVD, or USB drive) only with the specific authorization of the appropriate college vice president identified above and the Vice President for Information Systems. The college employee in whose custody such portable storage system is entrusted shall be responsible for protecting that data from compromise as well as encrypting all data on said devices.
6. Data files containing PI considered sensitive data shall not be transferred or downloaded to portable storage media except with the authorization of the College President on the advice of the responsible college vice president/administrator identified above and the Vice President for Information Systems. The approval must document the business reasons for accepting the risks to the data and a description of the mitigating controls in place. All data storage media containing sensitive data must be both physically and logically secured by means approved by the Vice President

for Information Systems. The college employee in whose custody such portable storage system is entrusted shall be responsible for protecting that data from compromise. Appendix E provides the format for requesting authorization to store sensitive PI data on portable storage media and approval thereof. All data transferred or downloaded must be encrypted.

7. Authorized data files that contain PI and that need to be shared with other employees in the conduct of their assigned job responsibilities will be stored in a "shared directory" such that access is controlled through the college's centrally managed network security procedures.
8. Data containing PI will not be posted to the college's Internet websites. Data containing PI posted on the college's SharePoint site will be encrypted.

Department heads and responsible departmental personnel must continually assess the vulnerabilities of their electronic as well as paper-based systems. Annually, in July, each department with responsibility for collecting, processing, or storing PI will assess the safeguards in place to protect that sensitive data. A report of this assessment will be submitted to the respective supervising member of the President's Executive Staff who will review and submit the report to the College Privacy Officer by August 1st of each year. Specific safeguarding practices that departments must assess, and if necessary, implement, and include in employee training, include:

1. Maintaining physical security by locking rooms and file cabinets where PI is stored or electronic storage is housed. Procedures should include ensuring that windows and doors are locked when areas are unoccupied and restricting access to areas where sensitive data exists.
2. Maintaining adequate key control and limiting access to sensitive areas to those individuals who require access to the area to carry out their assigned job duties.
3. Using authentication processes (such as secure passwords) and granting access privileges only to authorized personnel with legitimate business need to authorize and enforce a user's access to and actions towards specified resources.
4. Using firewalls and encrypting information when feasible.
5. Referring calls and mail requesting PI to those individuals who have been trained in safeguarding information.
6. Shredding paper documents containing PI.
7. Encouraging employees to report suspicious activity to supervisors.
8. Ensuring that agreements with third-party contractors who have access to PI collected by the college contain safeguarding provisions and monitoring those agreements to oversee compliance with appropriate privacy and safeguarding measures.
9. Ensuring that electronic hardware, electronic operating systems, software upgrades and other electronic means of storing and manipulating data are installed and configured to maintain adequate security of PI.

4.2. Compromise of Personal Information

Whether the Personal Information is maintained in a paper- or computer-based storage system, it will be considered to have been compromised when the security of the system in which it resides is breached. A paper-based information storage system may be considered to have been compromised when a person not authorized to have access to the sensitive data contained in the system gains such access. A computer security breach is any incident in which the security of a computer system is compromised, including theft or loss of a computer or storage device or medium where unauthorized person(s) might have been able to access, copy, or read data files on it. It does not include normal business use by authorized employees or third-party business partners of the college authorized to receive and process PI collected by the college. See “Breach [Computer System] on page 13 for the legal definition from the *Code of Virginia* § 18.2-186.6.

Compromise of Personal Information falls into three categories: incidental, accidental, and intentional.

4.2.1. Incidental Disclosures

Incidental Disclosures are unintended revelations of Personal Information that occur during an otherwise permitted use or disclosure of the information. For example, an employee steps into the supervisor’s office and begins discussing a personal matter before the supervisor can shut the office door, and another employee waiting to meet with the supervisor inadvertently overhears a portion of the discussion.

An Incidental Disclosure is usually not reportable as a Privacy Incident, and an authorized holder of PI who takes reasonable precautions to preclude its disclosure will not be held responsible. However, professional judgment should be used to assess the potential outcome(s) of an Incidental Disclosure. Any disclosure that may result in fraudulent or criminal misuse of the information or have a negative impact on TCC must be reported immediately to the College Privacy Officer.

4.2.2. Accidental Disclosures

Accidental Disclosures are unintended exposures of Personal Information despite proper procedures having been followed. For example, a vehicle transporting documents containing Personal Information is involved in an accident resulting in a box containing some of the documents being dislodged and falling open with some pages being blown away. Accidental disclosures are Privacy Incidents and must be reported immediately to the College Privacy Officer.

4.2.3. Intentional Disclosures

Intentional Disclosures are disclosures of Personal Information that occur due to disregard of established policies and procedures, with or without

malicious intent. For example, disclosing Personal Information to another individual without confirming that person's identity or authority to have access to the information disclosed.

Any member of the TCC community who becomes aware of an Intentional Disclosure of Personal Information is obligated to report the incident immediately to the College Privacy Officer. Intentional Disclosures are Privacy Incidents and will result in counseling or disciplinary action. Distinct from any sanction imposed by the college, an Intentional Disclosure may also result in personal liability, either in civil or criminal legal action.

4.3. Reporting Policy Violations

4.3.1. Reporting Compromise of Personal Information

Any member of the college community who becomes aware of an unauthorized disclosure or acquisition of Personal Information or suspects that such an incident has occurred should first take steps to correct the situation. For example, recover a document left in a public place; shut down the affected computer, server, or network; or lock the door to an area where Personal Information has been left exposed.

Following the immediate action to protect the Personal Information, the person who has become aware of the situation should complete and submit a Privacy Incident Report form (Appendix F) as soon as practicable, but no later than the end of the person's work- or class-day. The report will be submitted to the College Privacy Officer and to the respective college vice president/administrator with cognizance over the type of information involved in the incident. If the incident involves a computer or other college information technology resource, the report will also be submitted to TCC's Information Security Officer.

After investigation of the incident, if notification of affected persons or mitigation is required, departments and/or individuals involved in the privacy breach may be asked to assist with the notification process and/or in mitigating effects of the condition that caused the incident.

4.3.2. Reporting a Privacy Complaint

Any individual who believes that his/her privacy rights have been violated may file a complaint with TCC by completing and submitting a Privacy Complaint form (Appendix G) to the College Privacy Officer. An initial report may be filed with the College Privacy Officer verbally or by written communication other than the college's form. However, the complainant or a designated representative must file the complaint form in order to establish a formal complaint with the college.

The College Privacy Officer or designated representative will make every effort to contact the individual filing the complaint within three (3) business days of receiving notice of the complaint.

Following investigation of the complaint, the College Privacy Officer will notify the complainant of the results of the investigation and the corrective actions to be taken, if any.

4.4. Investigating and Responding to Compromises of Personal Information

4.4.1. Privacy Incidents

The College Privacy Officer or designated representative will:

1. Initiate a formal investigation immediately upon receipt of a report of a Privacy Incident. The person notifying the College Privacy Officer should complete a Privacy Incident Report form for this purpose. Determine whether the person(s) whose information is involved is aware of the alleged incident.
    a. If the person(s) is/are aware of the incident, contact him/her/them within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the College Privacy Officer. Document the contact, and include the date, time, and a general summary of any conversations or messages left or received.
    b. If the affected person(s) is/are not aware of the privacy incident, investigate the alleged incident thoroughly and contact the person(s) affected.
2. Advise the College President and the respective vice president/administrator with cognizance over the information involved in the incident of the results of the investigation and any recommended actions.
3. File the completed Privacy Incident Report with all investigation and resolution documentation in the College Privacy Officer's files. (Documentation of the investigation will not be included in an affected person's employee or student records.)
4. Maintain all documentation for at least six years.

4.4.2. Privacy Complaints

The College Privacy Officer or designated representative will:

1. Initiate a formal investigation immediately upon receipt of a complaint of a violation of an individual's privacy, whether the complaint is made verbally or in writing.
2. Contact the complainant within three (3) business days of receiving notice of a complaint.

a. Advise the complainant of the investigation process.

b. Request any clarification regarding the complaint that may be needed to facilitate the investigation.

c. If not already done, request that the complainant complete and submit the Privacy Complaint form to formalize the complaint.

d. Document the conversation, including the date, time, and a general summary of the conversation.

3. Advise the College President and the respective vice president/administrator with cognizance over the information involved in the incident of the results of the investigation and any recommended actions.
4. Attach any relevant materials or statements to the investigation documents.
5. File the completed Privacy Complaint form along with all investigation and resolution documentation in the College Privacy Officer's files. (Documentation of the investigation will not be included in an affected person's employee or student records.)
6. Maintain all documentation for at least six years.

4.4.3. Response When No Compromise Is Found

If, after investigation of a reported incident or a complaint, the College Privacy Officer determines that no compromise of Personal Information occurred, the following actions will be taken to close out the matter.

1. The findings and any recommended actions will be documented in the investigation report which will be maintained on file for at least six years.
2. Appropriate notification of will be provided to the person(s) whose Personal Information was involved.

   a. For Privacy Incidents where no compromise is found, notify the person(s) whose information was involved only if they were already aware of the potential compromise. Document any conversations, and provide written records of the incident resolution, as appropriate.

   b. For Privacy Complaints where no compromise is found, notify the complainant upon conclusion of the investigation and explain the findings; provide a written record of the complaint resolution.

4.4.4. Response When a Compromise Is Found

If, after investigation, the College Privacy Officer determines that a compromise of Personal Information has occurred, the following actions will be taken to close out the matter.

1. The findings and any recommended actions will be documented in the investigation report which will be maintained on file for at least six years. The Privacy Oversight Committee will be convened to recommend a corrective action and recovery plan, including any plans for mitigation, where appropriate.
2. Notification of affected individuals will be undertaken as delineated below.
    a. For Privacy Incidents, the College Privacy Officer will assist the college vice president/administrator with cognizance over the type of information involved to notify all persons whose Personal Information was compromised as soon as is practicable. Appendix H provides guidance on the notification process. Any subsequent conversations with the affected individuals will be documented. Written records of the incident resolution will be provided to the affected individuals, as appropriate.
    b. For Privacy Complaints, the College Privacy Officer will contact the complainant, explain the findings and any corrective actions to be taken, and provide a written record of the complaint resolution.
3. The College Privacy Officer will notify appropriate TCC staff of the confirmed compromise, including the Chief Communications Officer, the Director of Materiel Management (Risk Management), the Information Security Officer (if a breach of a computer system is involved), the supervisor of any employee determined to be at fault or the campus dean of student services if a student is found to have caused the compromise, and the member of the President's Executive Staff responsible for the area in which the compromise occurred.

5. Definitions

Breach. An actual violation of policy or procedure; going against established rules. Also, an unlawful and unauthorized acquisition of data that materially compromises the security, confidentiality, or integrity of Personal Information maintained by an entity.

Breach [Computer System]. The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the

individual or entity or subject to further unauthorized disclosure. (*Code of Virginia* § 18.2-186.6)

Compromise. Access in excess of that intended to be available.

Information system. The total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject. (*Code of Virginia* § 2.2-3801)

Mitigation. To make less severe, to partially remove, or to correct, so that harmful effects of a privacy violation are reduced or eliminated.

Notification. The act of informing persons affected by a breach of Personal Information that their information was included and steps they can take to protect themselves and their privacy.

Personal Information. All information that (i) describes, locates or indexes anything about an individual including, but not limited to, their social security number, driver's license number, real or personal property holdings derived from tax returns, and their education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or (ii) affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of their presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information. (*Code of Virginia* § 2.2-3801)

Privacy Complaint. An allegation by an individual that an organization is not complying with the requirements of the federal privacy and/or security regulations or the organization's own policies and procedures related to the privacy / security of personal information.

Privacy Incident. A known or suspected action, inconsistent with the college's privacy policies and procedures, or an adverse event, related to restricted or sensitive information.

Sensitive Data. Data which, if compromised with respect to confidentiality, integrity, or availability, could adversely affect the Commonwealth's interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data are classified as sensitive if compromise of that data results in a material and significant adverse affect of the Commonwealth's interest, the inability of the affected agency to conduct its business, and breach of privacy expectations. (COV ITRM Guideline SEC507-00)

6. References

Government Data Collection and Dissemination Practices Act (*Code of Virginia* § 2.2-3800 *et seq.*)

The Virginia Freedom of Information Act (*Code of Virginia* § 2.2-3700 *et seq.*)

Information Technology Data Protection Guideline (COV ITRM SEC507-00)

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 *et seq*.).

Fair and Accurate Credit Transactions Act (FACT Act) (16 C.F.R. Part 681.

Financial Services Modernization Act (Gramm-Leach-Bliley Act) (15 U.S.C. § 6801 *et seq*.)

Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)

Information Technology Resource Management Guideline: Internet Privacy Guidelines

7. Review Periodicity and Responsibility

The College Privacy Officer shall review this policy at each anniversary of its approval and, if necessary, recommend revisions.

8. Effective Date and Approval

The revision of this policy is effective upon its approval by the College President on March 29, 2018.

Policy Approved:	Procedure Developed:
Edna V. Baehre-Kolovani, Ph.D. President	Christine Damrose-Mahlmann, Ph.D. Privacy Officer

9. Review and Revision History

The initial version of this policy was approved on June 4, 2010.

This is the first revision of this policy. This policy replaces and supersedes the previously implemented Policy on Protecting Personal Non-Public Information.

- Revision 1 updates the policy to add more specific language related to 1) sanctions for failure to comply with security measures; and 2) the process of removal of social security numbers. These were the suggestions of legal council for the VCCS.

This policy was approved on January 18, 2017.

This is the second revision of this policy. The policy replaces and supersedes the previously implemented Policy on Privacy.

- Revision 2 updates the policy to 1) change to gender neutral language; 2) provide clarity in the language concerning the use of PI and SIS numbers; 3) identify the Information Security Officer as the backup to the Privacy Officer; 4)

specificity of the responsibilities of the Privacy Oversight Committee; 5) update titles of responsible individuals; and 6) update forms for appropriateness.

This policy was approved on March 29, 2018 by President Edna V. Baehre-Kolovani, Ph.D.

APPENDIX A

TIDEWATER COMMUNITY COLLEGE

INFORMATION PRIVACY STATEMENT

Commitment to Privacy

Tidewater Community College values each individual's privacy and actively seeks to preserve the privacy rights of those who share information with the college. The trust of the college's constituents is important to TCC, and those constituents have the right to know how information submitted to the college is generally handled.

The following privacy notice is provided to define TCC's information policy and practices, and to assist the college's constituents in protecting their privacy.

Privacy Notice

TCC has adopted the following privacy policies and practices for any and all parts of the college where **Personal Information (PI)** in any format is created, received, maintained, and transmitted. However, in legal terms, this notice shall not be construed as a contractual promise, and the college reserves the right to amend its policies at any time without notice. Privacy and public records obligations of the college are governed by applicable Virginia and federal laws and regulations.

Personal Information (PI)

The legal definition of Personal Information is provided in *Code of Virginia* § 2.2-3801 and is included in TCC's policy on Privacy. For practical purposes, PI may be considered to be any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

1. Names and Numbers:
    a. Name (when combined with other elements of PI listed below)
    b. Date and year of birth
    c. Social Security number
    d. Mother's maiden name
    e. Official state-issued or US-issued driver's license or identification number
    f. Alien registration number
    g. Government passport number
    h. Employer or taxpayer identification number
    i. Medicaid or food stamp account number
    j. Bank account number
    k. Credit or debit card number
    l. Personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;
2. Unique biometric data, such as fingerprint, voiceprint, retina or iris image, or other unique physical representation;

3. Unique electronic identification number, address, or routing code;
4. Medical records;
5. Academic grades;
6. Telecommunication identifying information or access device; or
7. Other number or information that can be used to access a person's financial resources.

The Information TCC Collects

When a constituent contacts TCC, certain client information may be collected. No information is collected unless the constituent deliberately provides it to the college (for example, by leaving a name and telephone number, by completing a college form, or by clicking a web-link to send an e-mail to the college). Examples of the information that constituents might choose to give the college are listed below:

- Name, address, telephone number, and e-mail address
- Names, addresses, telephone numbers, and e-mail addresses of family members and/or friends
- Date of birth, ethnicity, gender, and country of origin
- Height, weight, hair and eye color, and blood type
- Academic history, including schools attended, grades received, and test scores
- Financial profile, including income and assets
- Employment history, including previous employers and duties
- Credit or debit card and bank account information
- Criminal history, including convictions, time served, and probation status

The Way TCC Uses Information

As a general rule, TCC maintains various types of records for individuals based upon their association with the college. TCC also aggregates information for resource management and planning purposes. TCC reserves the right to use information details about individuals to investigate its resource management or security concerns.

Personal Information is used to accurately compile, store, and retrieve an individual's records; to place and track individuals appropriately for academic purposes, and to award academic degrees and honors; to properly employ individuals and compensate them for their work; to correctly diagnose and medically treat individuals; to respond appropriately (or in a personalized format) to individuals' requests for services; and to improve the college's services and products.

Under The Virginia Freedom of Information Act (FOIA), most records in the college’s possession are subject to inspection by or disclosure to members of the public upon their request. Information must be retained according to applicable federal and state laws, and must be available for inspection, unless otherwise exempt from FOIA.

TCC uses the PI provided by a constituent placing a request for service only to complete that order or request. The college does not share this information with outside parties, except to the extent necessary to complete that order or request.

TCC generally uses return addresses, telephone numbers, and e-mail addresses only to answer the communications received by the college. Such addresses are generally not used for any other purpose and by college and state policy are not shared with outside parties, except in accordance with FOIA.

Finally, TCC does not use or share the PI provided to the college in ways unrelated to the purpose described without a clear notice in advance and without also providing the constituent an opportunity to opt-out or otherwise prohibit such unrelated uses.

Providing Information is Optional

Except where otherwise provided by TCC policies and procedures for college employees, there is no legal requirement for a constituent to provide any information to TCC. However, most of the college's services and products will not be available without the essential relevant information being provided by the constituent.

TCC's Commitment to Data Security

TCC is committed to preventing unauthorized information access, maintaining information accuracy, and ensuring the appropriate use of information. The college strives to put in place appropriate physical, electronic, and managerial safeguards to secure the information it collects in all formats: on paper, electronically, and verbally. These security practices are consistent with the college's policies and with the laws and regulatory practices of the Commonwealth of Virginia and multiple federal agencies.

How to Contact Us

Should you have other questions or concerns about these privacy policies and practices, please contact TCC's College Privacy Officer at 757 822-1298. You may send written correspondence to the College Privacy Officer by e-mail at privacy@tcc.edu or by letter addressed to: College Privacy Officer, c/o Office of the President, 121 College Place, Norfolk, VA 23510.

APPENDIX B

TIDEWATER COMMUNITY COLLEGE

RESPONSIBILITIES OF THE COLLEGE PRIVACY OFFICER

Reporting to the College President, the College Privacy Officer will ensure institutional compliance with federal and state privacy regulations, as well as industry standards, for restricted information; and will provide centralized resources, oversight and enforcement for privacy-related activities.

Core responsibilities of the College Privacy Officer are:

1. To identify college functions, routines, business practices, and record repositories—electronic and physical—with privacy requirements, the risks associated with them, and the protective measures necessary to mitigate those risks.
2. To develop, implement, and maintain, in consultation with the college's administration, appropriate college-wide personnel and legal counsel, college-wide privacy-focused policies, procedures, and guidelines that comply with statutory mandates and industry regulations.
3. To serve as information privacy consultant to college departments/divisions in the development and review/modification of procedures and practices that have privacy implications, including information technology security procedures and practices under the purview of the Information Security Officer (ISO).
4. To oversee development of and ensure delivery of initial privacy orientation and continuing training to all employees.
5. To oversee development and delivery of information and promote activities to foster information privacy awareness among the college community, including students and visitors.
6. To oversee privacy program monitoring and enforcement as required by privacy statutes and standards through initial and periodic information privacy risk assessments and ongoing compliance monitoring activities in coordination with TCC's other compliance and operational assessment functions.
7. To serve as the college's central contact and investigation authority for privacy complaints, incidents, and breaches, including coordinating privacy notifications when required; to establish and administer a process for receiving, documenting, tracking, investigating, and taking action on complaints concerning TCC's privacy policies and procedures in collaboration with other similar functions and, when necessary, legal counsel.
8. To ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies by members of the college community, including students, in cooperation with the Associate Vice President of Human Resources or campus dean of student services, the Information Security Officer, department/division leadership, and legal counsel, as applicable.

9. To evaluate opportunities to reduce privacy risks and to recommend program modifications that advance overall privacy compliance.
10. To participate in the development, implementation, and ongoing compliance monitoring of business associate agreements, to ensure that privacy concerns, requirements, and responsibilities are addressed.
11. To establish, implement, and monitor mechanisms to track access to protected information within the college's purview and as required by law and to allow qualified individuals to review or receive a report on such activity.
12. To represent the college's information privacy interests, in collaboration with the cognizant member(s) of the President's Executive Staff, legal counsel, and other related parties, with external parties who undertake to adopt or amend privacy legislation, regulation, or standard.

APPENDIX C

TIDEWATER COMMUNITY COLLEGE

GUIDELINES FOR PROTECTING PERSONAL INFORMATION (PI)

Personal Information (PI) is that sensitive information about a person which, if compromised, would subject the individual to identity theft or other potentially severe negative effects. Examples of PI include, but are not limited to:

- Social Security numbers (SSNs)
- Credit card or bank account numbers
- Medical or educational records
- Other sensitive, confidential or protected data (e.g., grades used in context with personally identifiable information such as name, address, or other easily traceable identifiers).

The first step in protecting PI is to limit its collection and storage to only those instances dictated by law or support of essential college functions. Departments should review their processes for using PI annually:

- "Why are we acquiring SSNs or other PI?"
- "How are we storing any PI we do acquire?"
- "How are we protecting the PI that we acquire?"
- "What can we do to train our faculty and staff in the proper use and management of PI like SSNs, credit card numbers, and other confidential information?"
- "Who has access to PI in our department, and do they still need the access?"

In addition, if you are asked to provide a SSN or other PI (either your own, another employee's, a student's, a family member's), challenge the request to insure that it is based on a legitimate need.

The next step in protecting PI is to collect, process, and store it only on centrally managed systems (e.g., the Student Information System) that have appropriate security control measures in effect. **Unless specifically authorized to do so by the college vice president/administrator responsible for the data and the Vice President for Information Systems, you may not store PI locally.** "Locally" is defined as storing information directly on your college-owned computer.

You may not download or otherwise copy PI from the centrally managed system on which it resides to your local computer without specific authorization from the responsible college vice president/administrator and the Vice President for Information Systems.

You may not download to or otherwise store college data containing PI on a non-college owned system, such as your home computer, or to a portable computing system (e.g., a laptop), whether college-owned or not.

You may not download to or otherwise store college data containing PI on portable storage media without the specific authorization from the responsible college vice president/administrator and the Vice President for Information Systems. Storage of PI deemed to be sensitive data on portable storage media requires the specific authorization of the College President.

If you have been authorized to store PI on a portable storage system, such as a CD/DVD or USB drive, you are responsible for protecting the data from compromise.

When no longer required in support of college business, paper-based material containing PI shall be destroyed by shredding unless retention is required by federal or state law or regulation or by VCCS or college policy or procedure. Similarly, data containing PI shall be deleted from electronic storage media when no longer required for the conduct of college business.

Finally, wise management of information system resources, including controlling access to storage areas through appropriate security measures (e.g., controlling keys, using strong passwords, etc.) is an essential element of protecting PI. Should you become aware that the security of a data storage system (paper- or computer-based) may have been breached, immediately notify the responsible supervisor who will advise the appropriate college vice president/administrator.

APPENDIX D

TIDEWATER COMMUNITY COLLEGE

REQUEST TO ESTABLISH/MAINTAIN A LOCAL DATA FILE

CONTAINING PERSONAL INFORMATION (PI)

From: _____

To*: Vice President/Administrator for _____

Thru: (1) _____

(2) College Information Security Officer _____

Date: _____

Subj: Request to Establish Data File Containing Personal Information _____

I request authorization to establish/maintain a local data file (including an ad hoc query or report from a centrally-managed system) that will include Personal Information:

Database Name: _____

Purpose/Business Practice: _____

_____

PI Elements: ☐ Social Security Numbers ☐ Credit card/financial data
☐ Medical information ☐ Educational information
☐ Other: _____

Subjects: ☐ Students ☐ Potential Students ☐ Alumni
☐ Parents/Sponsors ☐ Employees ☐ Donors
☐ Other: _____

Source of Data: _____

Explain why a local data file must be maintained. _____

_____

Where will the data file be maintained? _____

Who will have access to the data file? _____

_____

How will access to the data file be controlled? _____

_____

How long will it be necessary to maintain the data file? _____

_____

Vice President/Administrator action: ☐ Approved** ☐ Denied

Signed: _____ Date: _____

* Student Affairs – student and alumni records (except SIS financial modules)
Associate Vice President– employee records
Finance – financial records (including financial aid and other financial modules in SIS)
Information Systems – infrastructure systems (e.g., GroupWise and voice-mail)

**Copies provided to: Vice President for Information Systems and College Privacy Officer

APPENDIX E

TIDEWATER COMMUNITY COLLEGE

AUTHORIZATION TO STORE SENSITIVE PERSONAL INFORMATION (PI)

ON A MOBILE DATA STORAGE MEDIUM

To: College President

From: Vice President/Administrator for

Vice President for Information Systems

Subj: Request to Store Sensitive Personal Information on a Mobile Data Storage Medium

We write to recommend authorization to store _____
Data to be stored

on a _____ by _____ for a
Data storage medium Individual(s) authorized to store the data

period of _____ from the date of approval. We recognize that the
Number of months – up to 1 year

data are sensitive and certify that the following business reasons require storing these data on a mobile medium.

1. _____
First business reason
2. _____
Second business reason
3. _____
Third business reason – add additional reasons, as required, on reverse

We further certify that the following physical and logical security controls will be put in place to mitigate the risk of storing these data on a mobile medium.

1. ☐ Physical ☐ Logical _____
First mitigating control
2. ☐ Physical ☐ Logical _____
Second mitigating control
3. ☐ Physical ☐ Logical _____
Third mitigating control – add additional controls, as required, on reverse

Submitted:	Signature	Date
Vice President for Information Systems		
Vice President/Administrator		

President's Action:		
☐ Approved as delineated above – I recognize that the data are sensitive and accept the risks of storage on the named medium with the mitigating controls in place.		
☐ Denied		

TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

APPENDIX F

TIDEWATER COMMUNITY COLLEGE

PRIVACY INCIDENT REPORT

Incident Date:	Incident Time:	Incident Location:
Name and Address of Individual Whose Personal Information Is Involved *(continue on reverse or attach list)*		
Nature of Incident:		
Harm or Negative Outcome:		Is the individual aware of the incident? ____ YES ____ NO If NO, do not inform the individual unless so instructed by the College Privacy Officer.
Persons Involved in This Incident		
Name	Title/Position	Can be reached at:
How was this person involved?		
Name	Title/Position	Can be reached at:
How was this person involved?		
Name	Title/Position	Can be reached at:
How was this person involved?		
Type of Information Involved: ____ Electronic Records ____ Paper Records ____ Other	Describe the Personal Information involved in as much detail as possible: ____ Name ____ Address ____ Phone #(s) ____ Social Security # ____ Bank Information ____ Credit/Debit #(s) ____ Birth Date Other Information—Please Describe:	
Who was notified of this Incident? (Names & Titles)		
Immediate Remedial Actions/Interventions, if any:		
Report Completed By (please print)		
Title:	Department:	
I can be contacted at or:		
Signature:		Date:

E-Mail using the Secure File Transfer method to: Privacy@tcc.edu

TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

APPENDIX G

TIDEWATER COMMUNITY COLLEGE

PRIVACY COMPLAINT

Today's Date: _____

Name of person making complaint: _____

Name of person whose Personal Information has been used or disclosed (if different from above)

_____

SIS #_____

I can be reached at: _____ or _____
Phone Number *Alternate Phone Number*

_____
Address: Street, City, State, ZIP Code

The best time of day to reach me is: _____

Type of Personal Information involved:

____ Health Information
____ Personal Identifying Information
____ Academic Information
____ Personnel Information
Other: _____

I feel that the privacy rights of the above-named person have been violated in the following way:

_____
_____
_____
_____
_____
_____

This is what I want done to resolve this violation:

_____
_____
_____
_____
_____

Signature: _____

E-Mail using the Secure File Transfer method to: Privacy@tcc.edu

APPENDIX H

TIDEWATER COMMUNITY COLLEGE

PROCEDURES FOR NOTIFICATION IN THE EVENT OF

COMPROMISE OF PERSONAL INFORMATION

The *Code of Virginia* § 18.2-186.6 and the Virginia Information Technologies Agency (VITA) Information Technology Security Standard (COV ITRM Standard SEC501-01) require notification of potential victims of compromise of Personal Information under certain circumstances. In cases of compromise of Personal Information not covered under the *Code* or SEC501-01, the College Privacy Officer will determine the necessity and method of notification using these procedures as a guide.

Under the *Code* and SEC501-01, notification is required when computerized data that contain the following Personal Information elements are compromised and when the data elements are neither encrypted nor redacted.

a. the first name or first initial and last name in combination with and linked to any one or more of the following data elements;
b. Social Security number;
c. Driver's license number or state identification card number issued in lieu of a driver's license number;
d. financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; or
e. other personal identifying information, such as insurance data or date of birth.

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the information:

a. five digits of a Social Security number; or
b. the last four digits of a driver's license number, state identification card number, or account number.

The notification requirement does not apply to information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

In the event of compromise of PI as delineated above, TCC will provide appropriate notice to affected individuals in the event of compromise of unencrypted and/or un-redacted PI as delineated above by any mechanism, including, but not limited to:

a. theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
b. theft or loss of physical hardcopy; or
c. security compromise of any system.

Notice is also required if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules.

The notice shall be provided without undue delay as soon as verification of the compromise is confirmed, except if law-enforcement is notified and the law enforcement agency determines and advises the college that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

The notification will consist of:

a. a general description of what occurred and when;
b. the type of PI that was involved;
c. what actions have been taken to protect the individual's personal information from further unauthorized access;
d. a telephone number that the person may call for further information and assistance; and
e. what actions the affected individuals should take. The actions recommended should include monitoring their credit reports and reviewing their account statements.

The notification will be provide by one or more of the following methodologies, listed in order of preference:

a. written notice to the last known postal address in the records of the individual;
b. telephone notice;
c. electronic notice; or
d. substitute notice – if the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:
    i. e-mail notice if the e-mail addresses for the members of the affected class of residents are available;
    ii. conspicuous posting of the notice on the TCC website; and
    iii. notice to major statewide media.

If the notice must be provided to more than 1,000 persons at one time, TCC will notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C.§1681(a)(p), of the timing, distribution, and content of the notice.