Daytona State College
Written Information Security Plan

Purpose.
This written information security plan (WISP) describes Daytona State College’s (DSC) ongoing efforts to secure information related to students, employees and other customer constituencies who provide certain sensitive information to the College. The College is required by law, specifically the federal Gramm-Leach-Bliley Act (“GLBA”) and its accompanying Safeguarding rule, the Federal Trade Commission's "Red Flags" rule, the Family Educational Rights and Privacy Act (“FERPA”), the Health Insurance Portability and Accountability Act (“HIPAA”), the Payment Card Industry’s Data Security Standard (“PCI-DSS”) and the Florida Cybersecurity Standards (FCS) ATS 74-2 to implement administrative, technical, and physical safeguards to access, collect, distribute, process, protect, store, use, transmit, dispose of, and otherwise handle customer information. To implement this plan, DSC will:

1) Maintain, monitor, and test this plan
2) Designate a security officer to coordinate the safeguarding of customer information
3) Identify and assess risks to the security, confidentiality, and integrity of constituent information
4) Evaluate, improve, and implement safeguards to protect constituent information
5) Oversee service providers/contractors with access to constituent information
6) Identify and respond to red flags concerning potential identity theft
7) Notify individuals of data breaches under circumstances established by law

This plan helps assure the College's ‘customers’ that the College is taking adequate steps to protect their information and to minimize loss in the event of a security breach. The plan also serves to deter and respond to an increasingly common crime nationwide – Identity Theft.

Scope.
The security plan protects information pertaining to the College community including students, employees, and other appropriate constituent groups, College-wide in any office, department, school, or responsibility area that is engaged in financial activities, maintains related customer information or other activity. In addition to full- or part-time employees and students, the plan scope includes contract and temporary workers, hired consultants, interns, student employees and certain contracted 3rd party vendors. When in doubt as to whether a school, department, responsibility center, or office is engaged in financial activities or other protected activities, the department should err on the side of applicability.

“Customer information” means any paper or electronic record containing non-public personal information (NPPI) about an individual that the College, or its affiliates, handle and maintain. Customer information includes any personally identifiable information provided by students, employees or others in order to obtain a financial product or service from the College such as loan applications, credit card numbers, account histories, and related consumer information. It also includes data found in accounts where the College provides services and defers payment such as in a deferred tuition payment plan or financial aid loans.
College Department Responsibilities

A. Securing Information

Departments must continually assess the safeguards they have in place to protect not only customer information, but also all confidential College data. Heads of Departments should appoint a trusted and knowledgeable employee to oversee their individual safeguarding programs. Specific safeguarding practices that Departments must assess, and if necessary, implement, include:

1. Maintaining physical security by locking rooms and file cabinets where customer and sensitive information is stored. Ensuring windows are locked and using safes when practical for especially sensitive data such as credit card information, checks, and currency
2. Maintaining adequate key control and limiting access to sensitive areas to those individuals with appropriate clearance who require access to those areas as a result of their job
3. Using and maintaining secure passwords to access automated systems that process sensitive information and requiring identification before processing in-person transactions
4. Using firewalls and encrypting information when feasible and using authentication and passwords when creating new accounts
5. Referring calls and mail requesting customer information to those individuals who have been trained in safeguarding information
6. Shredding and erasing customer information when no longer needed in accordance with department and College policy and the law
7. Encouraging employees to report suspicious activity to supervisors and law enforcement authorities
8. Ensuring that 3rd party service providers/contractors are capable of maintaining appropriate safeguards for the customer information at issue prior to engagement
9. Ensuring that agreements with service providers/3rd party contractors contain safeguarding provisions and monitoring those agreements to oversee compliance
10. Discouraging the use of social security numbers, payment card information & other PII, then only using it in accordance with College Policy
11. Installing computer location software such as Computrace and using encryption on laptops and computers as deemed appropriate
12. Vigilantly look for and report signs of malware and reduce the promiscuous web browsing behaviors that tend to give them a foothold into systems
13. Cautiously inspect all web links before clicking on them as this is the primary method that Phishing scams use to steal account credentials and data
B. Training

1. Departments should ensure that all new and existing employees who are involved in activities covered under this plan receive safeguarding and red flags training. New users to the College’s Enterprise Resource Planning ("ERP") systems must receive the appropriate training (New User Training), security awareness training through the online security awareness training, and training for additional data access authority as handled by each department.

2. Ongoing semi-annual security awareness training for all staff and faculty will be administered by the College CISO, and encompass the areas covered by this document.

3. Department managers may request additional departmental face-to-face training by contacting the College CISO.

C. Monitoring and Detection

Departments must continually assess what types of information is received, stored and distributed and assess the vulnerabilities of their systems. The College’s Chief Information Security Officer is available to assist in assessing the effectiveness of their existing safeguards and in proposing improvements. The College Campus Safety department, who have qualified security specialists on staff, are available to discuss physical security issues. Campus Safety will also provide a security analysis for a requesting department. Departments should also identify particular red flags that may indicate identify theft. These include:

1. Receipt of alerts from consumer reporting agencies such as a credit freeze or notice that certain accounts may be susceptible to fraud.

2. Receipt of suspicious documents containing forged signatures or apparent alterations or an identification card with a photograph that does not resemble the owner of the account.

3. Receipt of suspicious information such as a PeopleSoft identification number that does not match the individual, or information that matches somebody else’s education records, or submitting a lack of required personal information after further request.

4. Unusual use of or other suspicious activity related to an account, such as recurring payment made to a student despite the student’s not registering for courses, or refunds at unusual times, a pattern of dropping courses.

5. Receipt of notices from victims, law enforcement agencies, or others such as College administrators that an individual’s information has been breached.

D. Managing Systems Failures and Handling Red Flags

1. The College acknowledges that no system is flawless. Nevertheless, immediate steps must be taken to correct any security incident. Departments must immediately report significant failures of their safeguarding system to the College’s Campus Safety, and CISO if the problem involves computer security, and to the related departmental manager. Affected customers may also need to be notified by College officials after the department consults with the designated departmental manager, College Campus Safety, and the Office of General Counsel about the necessity of notification and the proper notification procedures. See College Procedure 312(a) - IT Security Incident and Response and
Reporting. Examples of significant failures would include a successful hacking effort that results in the loss of unencrypted personal data as defined by Florida law, a burglary, or impersonations leading to the defrauding of customers.

2. Steps that Departments may take to respond to red flags if it has detected such or to prevent a potential loss of data include:
   a. Conducting an investigation
   b. Removing data from the network
   c. Monitoring accounts for evidence of identity theft
   d. Closing or re-designating accounts
   e. Refusing to open new accounts
   f. Contacting the customer after consultation with the aforementioned College officials
   g. Changing passwords and further enhancing physical or computer security after consultation with College Campus Safety or the CISO

E. No Third-Party Rights

While this plan is intended to promote the security of information, it does not create any consumer, customer, or other third-party rights or remedies, or establish or increase any standards of care that would otherwise not be applicable.

College Policies and guidelines that Protect Customer Information

The following policies and guidelines supplement and help to create a comprehensive written information security plan. Referral and adherence to these documents is imperative to the overall protection of customer information. The following documents are part of and are incorporated by reference into the plan.

A. College Policy 3.07 and Procedure 307 govern “Privacy of Student Records.” The policy and procedure outline the College's implementation of the Family Educational Rights and Privacy Act (FERPA). They can be found at:

B. The College's Registrar maintains an easy to read interpretation of FERPA as it applies to students' accounts at: https://www.daytonastate.edu/recreg/ferpa.html
   a. FERPA Training is conducted upon departmental request and each term through the Office of Human Resources and Information Technology department. The annual training is included in a FERPA module within the online security awareness training program. Additionally, the college conducts face-to-face training annually for faculty and staff during spring, fall, and summer.
   b. The Faculty Guidelines also speak to the interpretation of FERPA: http://library.daytonastate.edu/faculty/FERPA
C. College policy delineates the requirements and implementation of the Health Insurance Portability and Accountability Act (HIPAA). This policy bolsters patient privacy in regard to health care and can be found at:
   a. [https://www.daytonastate.edu/employee_benefits/files/Privacy%20Policy%202016.pdf](https://www.daytonastate.edu/employee_benefits/files/Privacy%20Policy%202016.pdf)
   HIPAA training is conducted through an on-line security awareness module as well as a face-to-face training for those areas that deal with Protected Health Information (PHI.)

D. The College stresses information technology security in the following policies and guidelines:
   a. College Procedure 312 “Network Internet Use” governs access to data: [https://falconmaildaytonastate.sharepoint.com/sites/it/DOCM/Documents/Departments/President%E2%80%99s%20Office/College%20Procedures/05-04-17%20DSC%20Procedures.pdf](https://falconmaildaytonastate.sharepoint.com/sites/it/DOCM/Documents/Departments/President%E2%80%99s%20Office/College%20Procedures/05-04-17%20DSC%20Procedures.pdf)
      and this is supplemented by role-based authorizations and training for the PeopleSoft student administration program
   b. College Procedure 312 also governs the security and privacy of College data and provides for disciplinary action against violators of the policy
   c. College Procedure 309 governs the use and management of social security numbers


F. College Procedure 312 emphasizes the protection and confidentiality of College information. It also specifically prohibits the misuse of information for personal gain or the gain of others in the Use and Misuse of Technology section.

G. The College maintains specific guidelines in the event of a security incident, how to respond and how to report. See College Procedure 312(a) - IT Security Incident Response and Reporting.

H. Additional procedures and guidelines related to Logical Access, Audit Logging & Monitoring, Security, and Application Management can be found in the IT Operations Manual

F. **Designated Chief Information Security Officer**

The Designated Chief Information Security Officer (CISO) reports to the Chief Information Officer, and is responsible for coordinating the safeguarding of customer information throughout the College. Per the requirements of the Red Flags Rule, the CISO shall report annually to the President and Senior Executive Staff on the College Departments’ adherence to this plan, effectiveness of the plan, serious incidents involving the use of the plan, related issues with third-party service providers, and any suggested material changes to the plan.
Security Guidelines

Physical Security

- File servers and PCs used in the administration of systems, should be kept in a secure room with restricted access. Be wary of potential access points such as windows, dropped ceilings, large air ducts, and raised floors. Server racks and machine cases should be locked when possible. The room should provide proper environmental conditions and safety for the equipment. Servers should not be placed directly on the floor in case of flooding. An approved fire suppression system should be kept in/near the server room.

- Physical security of hard copies and data storage media containing sensitive customer information must be maintained. Windows, doors, and file cabinets should be locked in areas where sensitive information is stored. Where feasible, safes should be used to store especially sensitive data such as credit card information, checks, and currency. Access control to sensitive areas must be maintained and limited to individuals who require access as a result of their job.

- High availability hardware should be used in all e-business servers (e.g. high quality components, redundant storage and power supplies, mirrored servers, error correcting memory, multiple NICs.) Uninterruptible power supplies should be used on all servers and tested regularly.

- Backups should be performed on a frequent and regular basis, and the backup media should be kept in a secure location. The backup media should be rotated and moved off-site as frequently as possible.

- Whenever possible, visible ports and exposed network cabling should not be present in vulnerable or public areas.

- Physical access to network communications closets in campus buildings should be considered secure with restricted access. These rooms should be environmentally controlled for the safety and operation of the equipment.
Data Storage

- DSC adheres to Payment Card Industry Data Security Standards (PCI-DSS) pertaining to storing, transmitting and processing credit card data. For questions about PCI-DSS, contact the CISO.

- Sensitive information, especially credit card data, should never be stored on the web server. The data collected by the web server should be passed to another physical machine for storage. Ideally, the data collected by an e-business web site should be stored in a location that is not directly accessible to the Internet. Sensitive information should be stored encrypted when possible. Be wary of sensitive data that may be stored in a web server’s cache or log files.

- The physical or electronic retention of sensitive information such as credit card numbers should meet appropriate compliance standards (e.g. PCI-DSS) and be avoided whenever possible. Sensitive information should be stored on the minimal number of machines while still maintaining system reliability. Care must also be taken to protect sensitive system data such as private keys.

- Sensitive information should be stored for a minimal length of time. The most sensitive portions of the information should be purged once it is no longer needed (e.g. deleting the customer’s credit card number once the transaction has been processed while retaining demographic information.)

- Copies of the data stored on the e-business machines must be treated with the same security precautions as the production data. Backup tapes and removable media must be kept in a secure location and sanitized or destroyed before disposal. Hard copies, such as reports, containing sensitive data should be stored in a secure location, and properly destroyed (e.g. shredded) when no longer required.
Data Transmission

- All transmissions of sensitive information between the web client and the e-business web server should utilize current industry encryption standards (e.g. 256-bit AES, TLS v1.2 encryption, with a minimal key length of 2048 bits) which are constantly evolving. File servers should be configured to refuse clients who cannot accept the required level of encryption, however, consider providing a link on the site so customers can download the required version of the browser. Usernames and passwords should not be transmitted over the network in clear text but rather encrypted. All administrative connections to the web server should also utilize encryption.

- Transmissions of sensitive information between machines other than a client and web server should utilize file encryption such as AES, and/or utilize a secure communication method such as VPN software, SCP, sFTP, or SSH.

- The transmission of sensitive information via e-mail should be avoided whenever possible. If e-mail transmission is necessary, data encryption should always be utilized (e.g. Office 365 email encryption, S/MIME.) Care must be taken to ensure that e-mail containing sensitive information is not stored, forwarded, or copied to insecure locations or unauthorized accounts. If sensitive information is retained on the mail server, then the mail server should be secured to the same standards as the e-business database server.
System Administration

- All e-business related servers must be hardened against cyber attack. Default installations of operating systems and many applications are rarely configured for ideal security. Minimal services should be running on the servers, and essential services must be properly configured and secured. Keep the least number of ports open on a system necessary for it to function properly, and close or filter traffic on all other ports. The servers should not be used for additional, unrelated applications, or used as a workstation. Patches and updates must be regularly applied, and manufacturers’ security recommendations and configurations should be removed when possible. Consider removing or disguising web server banners. Administrators should regularly monitor bug reporting and security sites for relevant security risks, and utilize scanning tools to check for vulnerabilities. All system configuration changes should be logged.

- System administrators must inspect log files (e.g. security, audit, firewall, antivirus) daily for suspicious activity, investigate repeated login failures, account management events, failed privilege use, policy changes, etc. Logs should have defined maximum sizes and retention periods. Administrators should periodically perform self-audits of the e-business systems. Staff should be informed of basic security practices (e.g. locking workstations, strong passwords) and be wary of social engineering attacks. Inquiries regarding customer information should be referred to individuals who have been trained in safeguarding information. Suspicious activity, including suspected intrusions and significant violations, should be reported to your supervisor, and College campus safety, and for cases involving computer security, the Chief Information Security Officer. Host and/or network-based intrusion detection systems should be considered as a further security measure.

- Strong passwords (preferably longer passphrases when possible) must be used for all user and system accounts. Enable passwords at multiple layers (e.g. BIOS, network login, database). Unattended machines should be kept locked with a password-protected screensaver. Inactive or unnecessary accounts should be disabled or removed. Default passwords, commonly known system accounts, or compromised passwords should be removed or changed immediately. Strong passwords should:
  o Have sufficient length to hinder brute force attacks (e.g. 8 or more characters)
  o Be changed on a regular basis (e.g. every 90 days)
  o Be unique and not reusable for a number changes (e.g. 6)
  o Be locked out after a number of failed login attempts (e.g. 50)
  o Not consist of dictionary words, proper nouns, or personally identifiable names or numbers (e.g. person’s name, computer name, SSN, phone number, birth date)
  o Make use of mixed case and non-alphabetic characters where possible
  o Be known only to the user responsible for the account (i.e. not shared with others)
  o Only used if a stronger authentication method (e.g. biometrics) is unavailable
  o When possible should be used in conjunction with multi-factor authentication

- Minimal system privileges should be granted to users and services, and file systems should restrict access to sensitive data. Rights should be granted on an as-needed basis. The use of privileged accounts should be kept to a minimum. Separation of duties should be implemented when
feasible. Ordinary user accounts should not be created on the e-business servers unless they are essential.

- File Servers and sensitive PCs should have systems in place to protect and detect malicious activities (e.g. run protective software such as antivirus or other endpoint protection software) that is kept up-to-date on an ongoing basis. Machines involved in the transmission or storage of sensitive information should reside behind a firewall or utilize router ACLs/IP packet filtering to restrict access.

- Disaster recovery and business continuity plans should be developed which include the definition of what constitutes a disaster, procedures of what should be done to recover from various failures, and how business will resume. The plan should be tested and periodically reevaluated. Data backups and restores should be performed on a regular basis. The backup and recovery process, including recovery point objectives and recovery time objectives, should be documented and tested on a regular basis. Consider how to handle service interruptions or a denial of service.
Application Development

- Strong user authentication (e.g. username/password, digital certificate) should be used with web-based systems. Unique user identification and passwords should be used and enforced by the application before each transaction. Passwords should not be visible or retrievable online. IP addresses should not be considered reliable authentication for sensitive information. Consider the use of personal digital certificates or tokens for stronger authentication.

- All user transactions should be logged with user ID, transaction type, data, time stamp, etc. Avoid logging unnecessary sensitive information. Care should be taken to ensure partial transactions do not occur in case of error or disruption of service. Consider how to handle non-repudiation issues and fraudulent transactions.

- Sensitive information should never be stored on the web server. Sensitive information should not be stored in persistent cookies. Cookies should not be considered a reliable authentication mechanism for sensitive information (e.g. reading a customer’s user ID from a cookie without password authentication). The acquisition of unnecessary sensitive information should also be avoided, such as storing customer social security numbers only for use as a primary key in the database.

- Ensure that no sensitive information, including login dialog, is being transmitted over the web without encryption. Session keys should automatically expire after a short period of time (e.g. ten minutes). Care should be taken to ensure that session ID algorithms are strong enough to avoid prediction or duplication of IDs. HTML pages should prevent encrypted files from being cached on the client via Meta tags.

- The transfer and display of complete credit card numbers or other sensitive information should be kept to a minimum. Credit card numbers should not be retrievable online. Applications should only display a small portion of the credit card number after it is initially entered by the user. Changes and deletions of the stored credit card number should be allowed without revealing the original number. For questions regarding PCI-DSS contact the CISO.

- Source code must be kept in a secure location. Store scripts and applications in a separate directory from mainstream content, or on a separate application server when possible. Programs and sensitive information should not reside in an area that can be indexed or readable by the public. Shield appropriate HTML pages from search robots with Meta tags or through dynamic content. Do not store scripting executables (e.g. Perl) in the CGI-Bin area. Do not store development tools such as compilers on production servers. When appropriate, a code escrow should be used.

- Many ways exist for unauthorized users to run code of their choosing on servers. All data provided by the user should be filtered and validated by several criteria (e.g. ranges, lengths, authorization, invalid characters) on both the client and server side to avoid buffer overflows. Avoid use of UNIX shell scripts where possible. Avoid programs that create temporary files to avoid possible system race conditions. Likewise, CPU time limits should be placed on scripts and applications. Avoid hard coded data values such as credentials and backdoors whenever possible.
• Ensure that all applications use proper HTML and coding to avoid complications, system crashes, and possible security risks. Mobile code should be signed to allow compatibility with secure clients. Consider how to handle clients who refuse or restrict the use of potentially insecure features such as cookies, Java, and ActiveX. Avoid use of relative paths when referencing commands or files. Avoid use of the “put” HTTP method; use the “post” method instead.

• Embedded scripts, cookies, “hidden” fields, search features, code comments, error messages, and URL lines can reveal sensitive information, programming structure, and possible security holes. Return codes should be checked and handled. Care should be taken to ensure that information sent to the browser does not reveal excess information about the system’s architecture, data validity, or any sensitive information. Do not transmit unnecessary parameters.

• Online content and program modifications should follow an established change control procedure with testing. Test results should be retained. All code should be reviewed by multiple competent developers. Content should be inspected to avoid copyright or trademark infringements, defamatory statements or privacy infringements. Consult with the Office of General Counsel, to determine whether a copyright notice, legal disclaimer, and/or privacy statement is needed on the web site. Broken or orphaned links should be removed or corrected.

• Applications and modifications should be thoroughly tested before being placed online. Use tools to check for common errors such as buffer overflows and code syntax. The access of the application from various browsers must be tested for compatibility. The system should be tested for reliable service under projected production loads and stress conditions.

• Security should be of paramount importance from the inception of the application development process, not something that is added later. It should be at the forefront of considerations from the first line of code, not some phase of development that is visited after the application is built.