Data Integrity & Security Overview & Guidelines

Washington State Community College

October 24, 2016

Internal/Staff Use Only

Data Integrity & Security Overview & Guidelines

Washington State Community College

Purpose of this document

The purpose of this document is to provide general guidance and guidelines for maintaining the integrity and security of Washington State Community College's operational data and related processes, as well as a general overview of existing efforts.

If you suspect a problem…

To report suspected or known problems, please submit a ticket to the Management Information Systems Help Desk by emailing PCService@wscc.edu, utilizing the Kinetic Agent on your WSCC issued PC, or calling extension 1178.

Table of Contents

Preventative Actions

Physical Security of Sensitive Data

Data Backups and Server Security

Ensuring Accurate Data Entry for Student Records

ETL Integrity Checks and Data Warehouse Security

Web Application Security

Accuracy of Reporting

Preventative Actions

Data Security and Integrity Begins with You!

Data security and integrity issues can affect all faculty, staff, and students of the college in very serious ways. The most effective tool to help prevent these problems in your day-to-day operations is care and concern for the information your office uses and creates. State and Federal laws and regulations apply strict controls of sensitive student data. More can be found at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html or by contacting the Registrar.

The following items represent proactive measures you should take to prevent the loss of sensitive data such as student records. For information on staying safe online, visit http://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Cyber-Safety/Cybersecurity.

Securing Your Work Environment

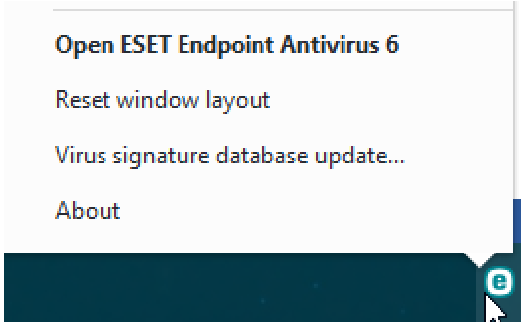
Your physical workspace represents an easy target for data thieves, hackers, and others who wish to gain unauthorized access to information. Keep in mind the following:

- **Never** leave sensitive information unsecured in plain view.
- **Never** write down passwords or other credentials near your work station.
- **Never** save passwords in a web browser autofill, as someone with access to that machine would then have access to those services.
- **Never** share your log in credentials with anyone. If you need assistance changing a password, unlocking account, or creating a new account for a user, please contact MIS at PCService@wscc.edu.
- **Always** utilize door locks, filing cabinet locks, and other physical security features to prevent unauthorized access to workspaces.
- **Always** lock your personal computer or other electronic devices when leaving your workspace. On Windows computers, this can be done by pressing Ctrl+Alt+Del and pressing enter.
- **Always** log out of secured resources when finished, especially on shared computers.

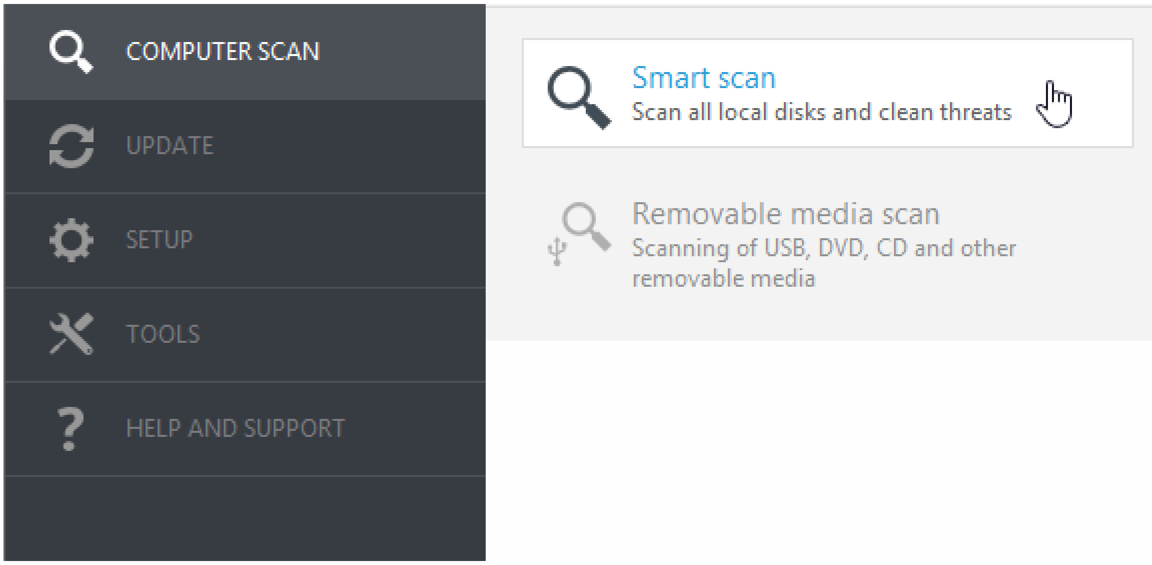
Antivirus Software

A common method for system intrusion to access sensitive data is through a virus or malware program. Infection often occurs through the opening of infected email attachments, the downloading of software from untrusted vendors, and similar vectors.

Your WSCC issued Windows device utilizes quality antivirus software through group policy. The antivirus signature database is updated automatically, and provides real-time scanning. If you wish to run an on-demand scan of your system, you may initiate it by right clicking on the ESET icon as shown on the following page and selecting Open ESET Endpoint Antivirus.


Open ESET Endpoint Antivirus 6
Reset window layout
Virus signature database update...
About

Once the antivirus has opened, select the COMPUTER SCAN menu option, and then select Smart scan as shown below.


COMPUTER SCAN
UPDATE
SETUP
TOOLS
HELP AND SUPPORT
Smart scan
Scan all local disks and clean threats
Removable media scan
Scanning of USB, DVD, CD and other removable media

If a virus or suspicious program is detected, or you suspect that your device may have been exposed to a virus or malware, please contact the Information Technology department through PCService@wscc.edu, the Kinetic Agent, or at extension 1178.

Operating System and Software Patches

Operating system and software vendors regularly publish security and bug-fix patches to improve your computing experience, and improve the security posture of the system.

While many of the common software applications used are automatically updated through group policy, installing these updates when they become available is very important to reduce your vulnerability to exploits or system instability. If you are unsure about how to update a particular piece of software, or have questions regarding an update, please contact Information Technology through PCService@wscc.edu, the Kinetic Agent, or at extension 1178.

Physical Security of Sensitive Data

Physical Security of Information Technology Systems

Washington State Community College takes its responsibility seriously to securely store and process student and staff data. All servers reside physically behind locked security doors in a climate controlled Network Operations Center (NOC), with access limited to specific personnel. Office and lab PC's must be protected from theft or other loss by keeping the doors locked to the room where they are housed when not being actively attended, and by preventing unauthorized individuals from obtaining physical access to them.

Given the rise in the use of college-issued laptops, and other portable devices, it is incumbent upon every employee to take steps to prevent the theft, loss, or release of sensitive information. Practical physical security steps you should take every day include:

- **Never** leave a PC, laptop, or other device containing work information unattended in your vehicle, bag, or otherwise unattended in a public space.
- **Never** leave student data in removable media such as USB drives, CDs, or external hard drives in an unsecured location.
- **Always** lock your office's external door when unattended by staff members.

If you suspect that a mobile device has been compromised, lost, or stolen, report it immediately to your supervisor and the Information Technology department at extension 1178.

Disposal of Physical Media and Paper Records

Properly disposing of sensitive student records, or other types of information is critical to maintaining information security. Physical media includes USB drives, computer hard drives, CDs, and any other physical digital storage method. **Do NOT** simply throw away this type of media if it contains student information or other sensitive data. Please contact the Information Technology department at PCService@wscc.edu, through the Kinetic Agent, or at extension 1178 to schedule a pickup of the media by an IT staff person for proper destruction and disposal.

For printed, or written student records/sensitive information that must be disposed of, locked shred bins are available in the Staff Break Room, Library, Arts & Sciences, as well as other locations. Consult your supervisor to determine which records must be securely kept for document retention purposes, as well as the department procedure for shredding these documents.

When in doubt as to whether or not information may be thrown away or must be shredded, please inquire with your supervisor.

Data Backups and Server Security

UNC Shares for all Windows Computer Users

Each domain user account has been mapped to a UNC share to allow "roaming" access to My Documents folder, regardless of the workstation used. This provides several benefits including automatic file backups, file loss prevention from a hard drive crash or other PC failure, and the ability to access your files from multiple workstations.

Users are highly encouraged to store important files in their mapped My Documents folder to take advantage of these benefits.

Backups, and Patches for Servers

Each server undergoes a snapshot backup multiple times per day to the on campus backup appliance, with nightly off-site secure backups taken to ensure disaster recovery capability with approximately one week of backups maintained at all times. Each Windows-based server has security and bug-fix patches applied automatically through group policy.

Student Information System Backups, Maintenance, and Patches

The College's student information system utilizes a variety of backups to ensure continued operation, and avoid the loss of student records. Local same-server backups are conducted nightly, with these stored on the network, as well as transported off-site to allow for disaster recovery. At least one week of backups are kept at a time to allow for individual file restoration in the case of corruption.

Student information server maintenance, and security / bug-fix patching is conducted on a weekly and monthly schedule under contract with Ferrilli. This contract also allows for a limited number of monthly hours for expert advice and assistance.

Ensuring Accurate Data Entry for Student Records

Student Application Process

Often, the first official interaction a student has with the College is the online application process. Ensuring data accuracy and integrity at this stage is critical to the incoming student's experience as they progress through the various entrance processes.

The application itself has a variety of internal "sanity" checks, such as ensuring the applicant's age and year of high school graduation is within a reasonable range, as well as preventing them from by-passing required questions based on previous selections.

Once the student has completed the application, it must go through the application approval process. Upon logging in to the administration portal, the system conducts an additional set of tests and checks to attempt to ensure the integrity of the entered information. These checks include:

- Comparing the entered SSN, birthdate, and last name with those already in the system to determine if it is a duplicate record.
- Assessing the applicant's high school status, and intention to take CCP courses to determine if they are a CCP, EEP, or PSEO student.

The individual processing the applicant must then edit the entered information as necessary, including fixing address capitalization or abbreviation issues, and then complete a check list of items before pulling the applicant into the student information system. Once an applicant has been pulled into the system, two automated emails are sent with a PDF acceptance letter, and another with additional MyWSCC information. These processes as well have embedded error checking and handling which will alert MIS and Student Services to a problem.

Transcript Import Process

Washington State Community College participates in the Ohio Department of Higher Education's Automated Transcript Clearinghouse (ATC) system, which enables the receipt and transmission of transcripts to and from Ohio's public colleges and universities. These transmissions are made securely to and from ODHE's servers, and are processed upon submission by the Records Office.

Before being pulled into the student information system, a significant number of checks are automatically done which not only attempt to automatically associate the information with the correct student ID, but as well will prevent the import from occurring if a problem such as a mangled transmission is detected. This prevents most issues related to the import of transcript information, and increases the reliability of this data.

Student Type Validation

A significant number of processes are associated with a student's type status, including tuition and fee billing. To reduce the number of errors and increase the efficiencies of the related processes, the Records Office conducts a variety of automated and manual checks to find students with expired, missing, or incorrect student types and fixes them prior to the beginning of each term.

This effort has reduced the number of incidents further down the chain, such as billing incorrectly or incorrectly identifying a student as CCP, in other departments significantly.

Military, Veteran, and Dependent Verification

Washington State Community College has made great strides in identifying, working with, and tracking the progress of military, veteran, and dependent students. Each veteran's record is examined and updated by the College's School Certifying Official, and the Management Information Systems department has developed several reports to assist in identifying erroneous military, veteran, or dependent records so they may be corrected.

ETL Integrity Checks and Data Warehouse Security

Kore Technologies Kourier ETL

As part of a previous effort to improve reporting capabilities, Washington State Community College has adopted an Extract, Transform, Load (ETL) software suite to assist in transferring data from the student information system's Rocket UniData files to SQL tables.

To ensure not only accurate reporting, but also the integrity of the source and destination databases, strict table schemas are utilized to prevent malformed records from being inserted. If a malformed record – such as the common issue of one with an invalid date – is attempted to be inserted, the insertion will be rejected and an automated email will be sent to the Management Information Systems department detailing the source record and the error. The MIS department will then contact the responsible department to seek a correction to this data.

Web Application Security

Use of Secure Socket Layer Technology

Web applications, such as the MyWSCC portal and online application, transmit data between a user and web server for processing and display. Encrypting this information in transit is critical to preventing man-in-the-middle, packet sniffing, and other types of cyber-attacks.

Each web server which transmits or receives sensitive information is outfitted with a SHA-256 security certificate to encrypt transmissions over the wire, meeting the Federal Information Processing Standards available here: http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4.

Reducing Attack Surface

As a standard operating procedure, the Management Information Systems department works to reduce the overall attack surface of the College's server infrastructure. This is done in part by removing unused or deprecated web applications from the production environment to present fewer possible vulnerabilities to a would-be attacker, as well as by maintaining the security patches on each web server and related software.

Additional steps are taken to prevent the defacement of College hosted websites, as well as regular backups taken to allow for a speedy recover in the event of an incident.

Logging and Monitoring

Each server maintains error, access, and request logs to assist technical staff with determining the source of issues, and to assist in discovering the source of any attempted network intrusions. These logs are monitored regularly, and proactive measures taken when possible to prevent network and server probing or attempted unauthorized access.

Preventing SQL Injection Attacks

One of the greatest risks to sensitive data in any web application environment is the possibility of a SQL injection attack. A successful attack of this nature can deliver sensitive data to the attacker, insert malicious data, or delete entire tables. Multiple layers of defenses are utilized to prevent such an attack, including the parameterization of SQL queries, the utilization of stored procedures, the sanitation of user entered data, and similar efforts.

Accuracy of Reporting

Processes for Verifying Generated State and Federal Reports

Providing accurate reporting for internal, state, and federal reports is one of the highest priorities of the Management Information Systems department. These reports can impact the institution's funding, and its performance on a variety of state and federal measurements. To ensure that the reports are accurate, each new report is presented the Data Action Team for review, modification, and approval after undergoing rigorous internal department testing.

Standard procedures for testing include the identification of a test pool of students which have particular varied types of data on their records, manually calculating the expected outcome, and comparing it to the automatically generated report. Subject matter experts from the requesting or impacted department(s) are also consulted at each step of development to provide additional information, input, and process explanation.

Data Action Team

Washington State Community College maintains a standing committee called the Data Action Team, which provides direction, oversight, and review of the diverse data sources, reporting, and software development projects undertaken by the College. It maintains representation from all functional areas of the institution, and meets monthly to conduct business.

Additional Resources

Federal Information Processing Standards: http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4
FERPA Regulations: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Ohio Attorney General Office of Cybersecurity: http://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Cyber-Safety/Cybersecurity
WSCC Key Performance Indicator website: https://kpi.wscc.edu/