WCU
WEST CHESTER UNIVERSITY

UNIVERSITY POLICY

Criminal History Record Information (CHRI) Proper Access, Use, and Dissemination Policy

Accommodations for individuals with disabilities in accessing these policies are available upon request by emailing accessiblepolicy@wcupa.edu

Purpose and Scope

WCU students engage in field, clinical, and practicum experiences (Experiences) that are an integral part of their WCU education. These Experiences are permitted by Affiliation Agreement between WCU and the Experience site. The Affiliation Agreement contains many terms that govern the Experience. This policy is regarding the criminal background reports that are required by the Affiliation Agreements. The intent of this document is to ensure the protection of Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with applicable record retention rules and to assure that CHRI is collected, stored, and disseminated in a manner that ensures accuracy, completeness, currency, integrity, security of such information, and to protect individual privacy.

The following standards were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. WCU may complement these standards with a local policy; however, the CJIS Security Policy shall always be the minimum standard. These procedures may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The scope of this policy applies to any electronic or physical (paper copy) media containing FBI CJI while being stored, accessed, disseminated electronically or physically moved from a designated secure location at WCU. CJI may only be accessed by authorized personnel. This policy applies to any authorized person who accesses, stores, and/or disseminates electronic or physical media. No unauthorized person may access CJI.

Policy Statement

Criminal Justice Information (CJI) and Criminal History Record Information (CHRI) are used interchangeably through this policy. Due to its comparatively sensitive nature, additional controls are required for the access, use, and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

Definitions

Criminal Justice Information (CJI): The term used to refer to all of the FBI CJIS-provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property, and case/incident history data.

Criminal History Record Information (CHRI): A subset of CJI and for the purposes of this document is considered interchangeable.

Physical Security: A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect FBI CJI and associated information systems.

Designated Secure Location: Applies to any electronic or physical (paper copy) media containing FBI CJI while being stored, accessed, disseminated electronically or physically moved from a designated secure location at WCU. CJI may only be accessed by authorized personnel. This policy applies to any authorized person who accesses, stores, and/or disseminates electronic or physical media. No unauthorized person may access CJI.

Electronic Media: "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Physical Media: "Physical Media" includes printed documents and imagery that contains CJI.

Media Transport: Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. WCU shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Overwriting (at least 3 times): As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

Degaussing: Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

Destruction: As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

Personally Owned Information Systems: A personally owned information system shall not be authorized to access, process, store, or transmit CJI.

Policy Framework

Proper Access, Use, and Dissemination of CHRI

WCU will not disseminate CHRI to any other agency. However, a Dissemination Log will be completed for all requests of dissemination from the designated secure location at WCU.

Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. Proof of training shall be kept on record.

Physical Security

Only authorized personnel will have access to physically secure locations. WCU will maintain and keep current a list of authorized personnel. All physical access points into WCU's secure areas will be authorized before granting access. Authorized personnel will take necessary steps to prevent and protect WCU from physical, logical, and electronic breaches.

Media Protection

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. WCU shall securely store electronic and physical media within physically secure locations. WCU shall restrict access to electronic and physical media to authorized individuals.

Media Sanitization and Disposal

When no longer usable, hard drives, flash drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store, and/or transmit FBI CJI shall be properly disposed of in accordance with measures established by CJIS.

Physical media shall be disposed of by one of the following methods:

1. Shredding using WCU issued shredders. Shredding must be completed by authorized personnel.
2. Placed in locked shredding bins for a private contractor to come on-site and shred, witnessed by authorized personnel throughout the entire process.

Electronic media shall be disposed of by one of the following methods:

1. **Overwriting (at least 3 times)**: An effective method of clearing data from magnetic media.
2. **Degaussing** – A method to magnetically erase data from magnetic media.
3. **Destruction** – A method of destroying magnetic media.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from WCU's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

WCU shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. WCU shall validate information system accounts at least annually and shall document the validation process.

All accounts shall be reviewed at least annually by the designated CJIS point of contact for each college (College Dean) or their designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information.

Remote Access

Publically Accessible Computer

WCU shall not authorize remote access to FBI CJI or the information systems that can access, process, transmit, and/or store FBI CJI. Access may only be obtained through WCU devices with secure internet access. Utilizing publicly accessible computers or interney to access, process, store, or transmit CJI is prohibited.

Utilizing publicly accessible computers to access, process, store, or transmit CJI is prohibited. Publicly accessible computers include, but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Personally Owned Information Systems

A personally owned information system includes any portable technology like cameras, USB flash drives, USB thumb drives, DVDs, CDs, air cards, and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops, or any personal desktop computer.

Reporting Information Security Events

All employees are required to report any incidents in which CJI documents are not disseminated in accordance with this policy, immediately to their Dean or Vice President.

Policy Violation/Misuse Notification

Violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel may constitute misconduct subject to disciplinary action, up to and including discharge or termination, in accordance with any applicable collective bargaining agreement provisions or State System or University policies.

Likewise, violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any unauthorized person may constitute misconduct subject to disciplinary action, up to and including discharge or termination, in accordance with any applicable collective bargaining agreement provisions or State System or University policies.

References

FBI CJIS Security Policy Title 28, Part 20, Code of Federal Regulations

PASSHE Policy Library

WCU Policy Library

Record Retention Rules

Reviewed by: Academic Contract Administration and Compliance Operations, Vice President for University Affairs and Chief of Staff, and University Legal Counsel

Policy Owner: Assistant Vice President, Academic Contract Administration and Compliance Operations

Approved by:

Mr. Andrew C. Lehman

Vice President for University Affairs and Chief of Staff

October 21, 2024

Effective Date: October 21, 2024

Next Review Date: October 20, 2029

Initial Approval: February 10, 2020

Amended: October 21, 2024