CRIMINAL JUSTICE INFORMATION PROTECTION POLICY

[FOR NON-POLICE DEPARTMENT EMPLOYEES]

1. Purpose

The purpose of this policy is to provide guidance for City personnel and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). It is also to ensure the protection of CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules. This Policy was developed and updated using the FBI's Criminal Justice Information Services (CJIS) Division's Security Policy 5.9.5, dated July 9, 2024. The FBI's *CJIS Security Policy* shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the FBI's *CJIS Security Policy* standards.

2. Scope

The scope of this policy applies to any electronic or physical media containing Criminal Justice Information (CJI) stored or accessed at the City, or physically moved from a City secure location. This policy applies to any authorized person who accesses, stores, and/or transports such electronic or physical media. Transporting CJI outside the City's assigned physically secure area must also be monitored and controlled in accordance with this policy.

3. Definitions

Authorized Personnel/User: An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI by the City.

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.

Escort: Authorized CJIS certified personnel who accompanies non-CJIS certified visitors at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein.

Local Agency Security Officer (LASO): City employee responsible for:

1. Identifying who is using the CJIS System Agency approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same;
2. Identifying and documenting how the equipment is connected to the state system;
3. Ensuring the approved and appropriate security measures are in place and working as expected; and
4. Establishing a security incident response and reporting procedure to discover, investigate, document, and report to the CJIS System Agency, the affected criminal justice agency, and the FBI CJIS Division Information Security Officer of major incidents that significantly endanger the security or integrity of CJI.

Terminal Agency Coordinator (TAC): City employee responsible for:

1. Ensuring that personnel security screening procedures are being followed as stated in this policy
2. Serving as the point-of-contact at the local agency for matters relating to CJIS information access.
3. Administering CJIS systems programs within the local agency.
4. Oversees the agency's compliance with CJIS system policies.
5. Is the City's contact for OSP/FBI audits.

Personally Owned Devices: A personally owned device is any technology device that was purchased by an individual and was not issued by the City. A personal device includes any portable technology like camera, 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. Threats to mobile handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services.

Physical media: Includes printed documents and imagery that contain CJI.

Physically Secure Location: 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 the FBI CJI and associated information systems.

Visitor: A visitor is defined as a person who visits City Hall on a temporary basis and has no unescorted access to physically secure locations within City Hall where FBI CJI and associated information systems are located. Visitors may include both City employees and non-employees who come to City Hall for business.

4. Policy

All physical, logical, and electronic access to CJI must be properly documented, authorized, and controlled on devices that store, process, or transmit unencrypted CJI. This Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

Under this policy, all personnel authorized with physical or logical access to CJI shall take all reasonable steps necessary to always protect and control electronic and physical CJI. As part of this obligation, the City will implement appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate

CJI disclosure and/or use must be reported to the City's Local Agency Security Officer (LASO) immediately following the event.

The following procedures are set-out to ensure secure accessing, handling, transporting, and storing of CJI.

5. Procedures

A. Media Storage and Access: Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed.

To protect CJI, Authorized City Personnel shall:

1. Store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Multi-Factor Authentication will be used for electronic systems that access, process, store, or transmit CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. Including overwriting data three times or degaussing prior to disposal.
5. Not use personally owned information systems to access, process, store, or transmit CJI unless the City has established and documented the specific terms and conditions for personally owned information system usage.
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the City in a secure area accessible to only those employees whose job function requires them to handle such documents.
8. Ensure only authorized users remove hardcopy printouts or digital media with CJI from physically secure or controlled areas.
9. Take appropriate action when in possession of CJI while not in a secure area:
    a. CJI must not leave the employees' immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
    b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of any physically secure location, the data shall be immediately protected using encryption (the cryptographic module used shall be certified to meet FIPS 140-3 standards).
10. Lock or log off computers when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.
11. Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI.

As this procedure pertains to a user's remote access to CJI:

1. The City shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store CJI. Remote access is any temporary access to an information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network.
2. The City shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The City shall control all remote accesses through managed access control points. The City may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access.
3. Any authorized user remotely accessing CJI must take necessary precautions when such access occurs outside of a physically secure area. Precautions include controlling any wireless network and service connectivity; validating mobile device default settings does not automatically connect to nearby Wi-Fi networks. Some of these networks, like in airports or neighborhood coffee shops, may be completely open and unsecured.

As this procedure pertains to a user's access of CJI through a personally owned device:

1. Per the City's Network User's Policy, the City does not permit personally owned devices to access, store, or transmit data on the city network, including electronic media containing CJI. The only exception is for allowing an employee's personal mobile or tablet device access to that employee's email mailbox utilizing the city's mobile device management software.
2. Where an employee may have inadvertent access to stored CJI through their email mailbox, the user must take precautions and follow necessary procedures to protect that CJI in compliance with this policy without exception.
3. If at any time, the City determines it is in the best interest to allow further or additional access to its network or information systems through personally owned devices, the City will take steps to implement greater procedural controls under this Policy.

B. 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.

City personnel shall:
Protect and control electronic and physical media during transport outside of controlled areas. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

City personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role-based rules for allowing access. Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
    a. Storing CJI in a locked briefcase or lockbox.
    b. Only authorized personnel can view or access the CJI electronically or document printouts in a physically secure location.
    c. For hard copy printouts or CJI documents: (i) Package hard copy printouts in such a way as to not have any CJI information viewable; and (ii) DO NOT MARK THE

PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)

5. Not taking CJI home or when traveling unless authorized. When disposing confidential documents, use a shredder.

C. Electronic Media Sanitization and Disposal: The City shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The City shall maintain written documentation of the steps taken to sanitize or destroy electronic media. The City shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. All physical media shall be securely disposed of when no longer required, using formal procedures.

D. Physically Secure Location for Access: Physically secure locations will be set out and designated within City Hall where CJI and associated information systems may be stored or accessed. The perimeter of any physically secured location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured at all times. Access points must remain closed and physically restrict non-CJIS certified individuals from entering the secured location.

E. Authorized Personnel Physical Access: Only authorized personnel will have unescorted access to physically secure non-public locations. The City will maintain and keep current a list of authorized personnel. Being authorized does not ensure proxy card access to all secure areas. Authorized personnel ID cards will identify authorization by a physical mark. The City will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.
    a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted for all personnel required to have CJIS access before assignment.
    b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.
    c. Refer to the *CJIS Security Policy* or the City's TAC for handling cases of felony convictions, criminal records, arrest histories, etc.
2. Complete security awareness training.
    a. All personnel with direct or physical access to CJI will receive security awareness training within 30 days of being granted duties that require CJI access and every year thereafter.
    b. Security awareness training will cover areas specified in the *CJIS Security Policy* at a minimum.
3. Be aware of who is in their secure area before accessing confidential data.

a. Take appropriate action to protect all confidential data.
b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
    a. Immediately report loss of issued keys, proximity cards, etc. to authorized agency personnel.
    b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the City's IT department to have authorized credentials like a proximity card de-activated.
    c. Safeguard and not share passwords, Personal Identification Numbers (PINs), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures.
5. Use of electronic media is allowed only by authorized personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.
6. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.
7. Report any physical security incidents to the City's LASO, including facility access violations, loss of CJI, laptops, smartphones, thumb drives, CDs/DVDs and printouts containing CJI. The TAC may be contacted if the LASO is unavailable.
8. Properly release hard copy printouts of CJI only to vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a “need to know” basis.
9. Ensure data centers with CJI are physically and logically secure.
10. Keep appropriate security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.
11. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped open, and take measures to prevent piggybacking entries.

F. Visitor Access: All Visitors must:
1. Be accompanied by an escort at all times. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort. Escort personnel will acknowledge being responsible for properly evacuating visitors in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures. Escort personnel will also validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.
2. Show City personnel a valid form of photo identification.
3. Not be allowed to view screen information, mitigating shoulder surfing.
4. Not be allowed to sponsor another visitor.
5. Refrain from taking any photographs or video, which are not allowed without permission of the visitor's escort.

Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be

asked to relocate to a non-restricted area. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in City Hall. In most instances, this duty will be carried out by the Front desk or Reception Desk.

G. Information Technology Support: In coordination with above roles, all vetted IT support staff will protect CJI from compromise by performing the following:
   1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted, and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, and internet connections as authorized by the City.
   2. Be knowledgeable of required technical requirements and policies, taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit, and at the end of life.
   3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using City approved best practices for power backup and data backup means, such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
   4. Properly protect the CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
      a. Install and update antivirus on computers, laptops, MDTs, servers, etc.
   5. Data backup and storage—centralized or decentralized approach.
      a. Perform data backups and take appropriate measures to protect all stored CJI.
      b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.
      c. Ensure any media released from the City is properly sanitized/destroyed.
   6. Access control measures.
      a. Address least privilege and separation of duties.
      b. Enable event logging of:
         i. Successful and unsuccessful system log-on attempts.
         ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
         iii. Successful and unsuccessful attempts to change account passwords.
         iv. Successful and unsuccessful actions by privileged accounts.
         v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
      c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
   7. Account Management.
      a. Ensure that all user IDs belong to currently authorized users.
      b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
      c. Authenticate verified users as uniquely identified.

d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
f. Passwords:
    i. Be a minimum length of eight (8) characters on all systems.
    ii. Not be a dictionary word or proper name.
    iii. Not be the same as the User ID.
    iv. Expire within a maximum of 90 calendar days.
    v. Not be identical to the previous ten (10) passwords.
    vi. Not be transmitted in clear or plaintext outside the secure location.
    vii. Not be displayed when entered.
    viii. Ensure passwords are only reset for authorized users.

8. Network infrastructure protection measures.
    a. Take action to protect CJI-related data from unauthorized public access.
    b. Control access, monitor, enable, and update configurations of boundary protection firewalls.
    c. Enable and update personal firewalls on mobile devices as needed.
    d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text.
    e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.
    f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
    g. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice department traffic using same wide area network.
9. Communicate and keep the City informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse.

H. Contract/Vendor agreements. In any occurrence where the city contracts with a vendor who will have access to CJI, they shall utilize the attached "Vendor Contract Addendum" and "Security Addendum" forms. Copies of these forms are auditable during both the OSP and FBI Audits. As such, copies of these forms in their final state shall be sent to the agencies TAC.

I. Breach Notification and Incident Reporting. All authorized personnel are responsible for reporting any unauthorized physical, logical, and electronic access of CJI. The point of contact to report any non-secure/unauthorized access is the City's LASO: IT Manager, Brian Miles, (503) 710-1370, Brian.Miles@ci.woodburn.or.us. In cases where the LASO is unavailable, you may contact the City's TAC: Police Support Services Sergeant, Shawn Hershberger, (503) 982-2352, Shawn.Hershberger@ci.woodburn.or.us. Reference the city's Incident Handling & Response plan for further details.

The City shall promptly report incident information to the CSO at Oregon State Police and/or necessary local entities. Security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

J. Penalties. Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution, and/or termination.

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization, or prosecution in the case of criminal activity.

6. Forms

CJI Protection Policy Acknowledgment
CJIS/LEDS SECURITY INCIDENT RESPONSE FORM
Vendor Contract Addendum Form
Vendor Security Addendum Form

7. References

The Federal Information Security Management Act of 2002
FBI Criminal Justice Information Services (CJIS) - Security Policy 5.9.5, dated July 7, 2024
FBI Criminal Justice Information Services (CJIS) – Security Addendum
28 U.S.C. 534

8. Review of Policy and Procedures

This policy will be reviewed every three years or as state and federal regulations are revised and necessitate a change in the policy or procedures.

Adopted: March 2025

CJI Protection Policy Acknowledgement

I have read the CJI Protection Policy and Rules and as an Authorized User, I acknowledge my responsibility to fulfilling that policy's requirements. Further, I agree to:

- Abide by the Policy. I understand any policy violation may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect the City's facilities, personnel, and associated information systems.
- Report any unauthorized physical access, breach, or network security incident to the City's LASO.

I understand that failure to sign this acknowledgment will result in denial of access to FBI CJIS systems, terminal areas, and facilities that have FBI CJIS network equipment.

Signature: _____ Date: _____

CJIS/LEDS SECURITY INCIDENT RESPONSE FORM

REPORTING FORM

DATE OF REPORT: DATE OF INCIDENT:

REPORTING PERSON:

PHONE/EXT/E-MAIL:

LOCATION(S) OF INCIDENT:

SYSTEM(S) AFFECTED:

METHOD OF DETECTION:

NATURE OF INCIDENT:

INCIDENT DESCRIPTION:

ACTIONS TAKEN/RESOLUTION:

PERSONS NOTIFIED:

VENDOR CONTRACT ADDENDUM

AMENDMENT NO. ___ TO THE CONTRACT BETWEEN

[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. ___ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "___"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions: a.

b.

c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _____, 20__. On behalf of [Party No. 1]: _____

[Name]

_____

[Title]

_____

[Date]

On behalf of [Party No. 2]: _____

[Name]

_____

[Title]

SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative