BACKGROUND AUTHORIZATION REQUEST FOR CONTRACTORS, VENDORS and NON-Criminal Justice Employees who have access to Criminal Justice Information Systems and/or facilities

Individuals who have direct or indirect access to the Criminal Justice Information Systems (LEIN/NCIC) shall submit to a background check prior to having unescorted access. This background check will include a state and federal fingerprint check. The Kalamazoo Department of Public Safety will determine, based upon state and federal guidelines, whether access will be granted.

By signing this authorization, the applicant grants permission to the Kalamazoo Department of Public Safety and any other public or private entity to conduct a background check for the express purpose of determining whether the applicant is eligible to access Criminal Justice Information Systems. The background search will include, but is not limited to, arrests, criminal charges, criminal convictions and information regarding criminal justice contacts.

I affirm that I have read and fully understand the above paragraphs and I consent to the aforementioned background check.

Signature _____ Date._____

Requested by			Date
Candidate for		Position	
Agency KDPS	☐ Temporary Employee	☐ Permanent Employee	☐ Contractor
Name of Candidate – Last	First	Middle	
Address		Apartment Number	
City		State	Zip Code
Social Security Number		Date of Birth	
Driver License Number		Sex ☐ Male	☐ Female
Race ☐ White	☐ Black (African)	☐ American Indian/Alaskan Native	
☐ Hispanic	☐ Asian/Pacific Islander	☐ Other	

THIS INFORMATION IS CONFIDENTIAL. DISCLOSURE OF CONFIDENTIAL INFORMATION IS PROTECTED BY THE FEDERAL PRIVACY ACT.

CONFIDENTIALITY AGREEMENT

I, _____ acknowledge that the nature of my duties while employed by Kalamazoo Public Safety or while working as a vendor or contractor at Kalamazoo Public Safety may afford me access to sensitive and/or confidential information and that by signing this agreement; I hereby agree to abide by the conditions of this agreement.

Criminal justice information and/or criminal justice information systems and their supporting networks are classified resources. As prescribed by law, access to criminal justice information and/or criminal justice information systems includes but is not limited to: network systems; routers and switches, applications and the data obtained from these resources are restricted to official business. Access requires authorization and a need to know. Authority to access this information can only be granted by the Chief of Police or his designee.

I have been briefed and fully understand that during the course of my duties I may become privy to criminal justice information and acknowledge that I am bound to protect this information at all times to include my separation from employment or service at Kalamazoo Public Safety.

Furthermore, I agree to protect the integrity of the information I may have become privy to from any criminal justice information resource and/or criminal justice information system in addition to the networks that support these networks and understand that by unlawfully accessing, acquiring or disclosing any information about this sensitive information, I will become subject to criminal prosecution in addition to any other penalties that are prescribed by law.

_____ _____

Signature **Date**

_____ _____

Witness Signature **Date**

Notary

State of Michigan County of Kalamazoo

Before me personally appeared the said _____
Who says they executed the above instrument of their own free will and accord and with full knowledge of the purpose therefore.

Sworn and subscribed in my presence the _____ day of _____ 20____.

My commission expires _____ _____

Notary Public

CITY OF KALAMAZOO
KALAMAZOO PUBLIC SAFETY
150 E Crosstown Parkway, Suite A
Kalamazoo, MI 49007

Personal Inquiry Waiver and Authority of Release of Information

Applicants Name:_____

Date/Place of Birth:_____

Social Security Number:_____-_____-_____

Applicant Authorization Consent for Release of Information
Please Read Carefully

We welcome your application with the City of Kalamazoo, Kalamazoo Public Safety. We require, as a condition of employment, that all applicants consent to and authorize a pre-employment verification of the background investigation submitted on their application, assessment questionnaire, and personal background questionnaire.

This release and authorization acknowledges that the City of Kalamazoo, Kalamazoo Public Safety may now or at any time while you are employed, conduct a verification on your education, personal references, motor vehicle records and to receive any criminal history records information pertaining to you which may be in files of any Federal, State or local criminal justice agency in Michigan or any OTHER state and/or other information as deemed necessary to fulfill the job requirements. The results of this verification process will be used to determine employment eligibility under Kalamazoo Public Safety employment policies. All results will be proprietary and will be kept confidential.

I, the undersigned applicant, do hereby release and consent and I authorize the background verification. I authorize all individuals, schools, current and former employers, financial or credit institutions and any other organizations and agencies to provide Kalamazoo Public Safety with all information requested and I hereby release all persons and agencies providing such information from any and all claims and damages connected with their release of any requested information. I agree that a copy of this document is as valid as the original.

I do hereby agree to forever release and discharge the City of Kalamazoo, Kalamazoo Public Safety and their associates to the full extent permitted by law from any claims, damages, losses and expenses or another charge or complaint filed with any agency arising from retrieving and reporting of information and acknowledge notice of right to receive a copy upon written request.

_____
Applicant's Signature

Must Be Notarized Before Returning

State of _____ County of_____

Before me personally appeared the said _____ who says he/she executed the above instrument of his/her own free will and accord and with full knowledge of the purpose therefore.

Sworn and subscribed in my presence the _____ day of _____, 20____.

My commission expires _____ _____
Notary Public

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
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).

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

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 CJA 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 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:

Assistant Director
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

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

Acceptable Access/Use of CJIS System/System Data Policy

1.0 Overview

The intention for publishing an acceptable access and use of CJIS systems/system data policy is not to impose restrictions that are contrary to Kalamazoo Public Safety's established culture of openness, trust, and integrity. Kalamazoo Public Safety is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, world-wide web browsing, File Transfer Protocol, and National Crime Information Center access are the property of the Federal Bureau of Investigation, Michigan State Police and Kalamazoo Public Safety. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every Kalamazoo Public Safety employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user and/or system's technician to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable access and use of CJIS system/systems and/or computer equipment at Kalamazoo Public Safety to risk including virus attacks, compromises of the network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporary staff, and other workers at Kalamazoo Public Safety, including all personnel affiliated with NCIC and third parties. This policy applies to all equipment that is owned, leased or accessed by Kalamazoo Public Safety.

4.0 General Use and Ownership

1. While Kalamazoo Public Safety's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the Kalamazoo Public Safety. Because of the need to protect Kalamazoo Public Safety's network, management cannot guarantee the confidentiality of information stored on any network device belonging to or use by Kalamazoo Public Safety.

2. Employees are responsible for exercising good judgement regarding the reasonableness of personal use. Individual departments are responsible for eating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absences of such policies, employees should consult their supervisor or management.

3. Kalamazoo Public Safety recommends that any information that a use considers sensitive or vulnerable to (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted. For guidance on information classification, refer to the CJIS Information Classification Policy.

4. For security and network maintenance purposes, authorized individuals within Kalamazoo Public Safety may monitor equipment, system, and network traffic at any time, per Kalamazoo Public Safety Audit Policy.

5. Kalamazoo Public Safety reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

4.1 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Please review the Service Division Password Policy for guidance.

3. All personal computers, laptops, and workstations should be secured with password-protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off (control-alt-delete) when the computer is unattended.

4. Because information contained on portable computers I especially vulnerable, special care should be exercised. Protect laptops in accordance with “Laptop Security Policy”.

5. All devices used by all employees/contractors that are connected to the Kalamazoo Public Safety Internet/Intranet/Extranet, whether owned by the Employee or Kalamazoo Public Safety, shall be continually executing approved virus-scanning software with a current database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.2 Unacceptable Use

Under no circumstances in a employee of the City of Kalamazoo, Kalamazoo Public Safety or contractor to either the City of Kalamazoo or Kalamazoo Public Safety authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing Kalamazoo Public Safety owned resources.

4.3 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Access to the Public Safety network and/or CJIS systems require authorization from the LASO (Captain of the Service Division). Unauthorized access, copying, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.).
2. Installation of any copyrighted software for which Kalamazoo Public Safety or end user does not have an active license or LASO authorization is strictly prohibited.
3. Installation of any software without preapproval and virus scan is strictly prohibited.

4. Introduction of malicious programs into the network or sever (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
5. Revealing your account password to other or allowing use of your account by others.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or login into a server that the employee is not expressly authorized to access, unless these duties are within the scope of a regular duties. For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited unless prior notification and authorization has been granted by the LASO.
8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network, or account/
10. Interfering with or denying service to any user other than the employee's host.
11. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
12. Providing information about NCIC or a list of Kalamazoo Public Safety employees to parties outside of Kalamazoo Public Safety.

5.0 Enforcement

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted dates. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

I have read, acknowledge, and will abide by the information obtained in this document. Furthermore, I agree to protect the integrity of the information I may have become privy to from any criminal justice e information resource and/or criminal justice information system in addition to the networks that support these networks and understand that by unlawfully accessing, acquiring or disclosing any information about this sensitive information, I will become subject to criminal prosecution in addition to any other penalties that are prescribed by law.

User (Print Name):_____ Date:

User Signature:_____ Date:

LASO/Security Officer:_____ Date:

Security Awareness Acknowledgment for Personnel with only Physical Access to Physically Secure Locations

I, _____, have read the following, or have had it read and explained to me, and understand and agree that:

My duties require me to work or be present in areas where Criminal Justice Information (CJI (may be seen. I realize that this information is sensitive in nature and will not discuss or reveal any CJI to anyone.

CJI refers to state and federal criminal justice date, which may include case/incident information, identity information (including fingerprints and other forms of biometric data), and property (such as vehicle or firearm) data.

Access to or sue of CJI (such as viewing, reading, copying, sharing) is strictly limited to official purposes, specifically the administration of criminal justice.

The term "administration of criminal justice" is defined in the CJIS Security Policy as:

> "Administration of criminal justice" means the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history records information; and criminal justice employment. In addition, administration of criminal justice includes "crime preventions programs" to the extent access to criminal history records information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and results of such checks will not be disseminated outside the law enforcement agency.

My work-related duties, as defined by my employer and understood by me, do not in any way involve the administration of criminal justice, as defined above.

In the course of my work-related duties, I may see or learn of (as by hearing mention of) CJI.

Because I have no responsibility or authority for handling CJI, I will not access, use, view, copy, disseminate, or disclose (in writing or in conversation) CJI, nor will I take part in the physical destruction of CJI. I am aware that doing so would e considered misuse of CJI.

I further understand that misuse of CJI is not limited to situations in which the CJI is used by me or the others for purposes or in a manner that could be punished under the criminal laws of the state or of the United States.

I acknowledge that misuse of CJI may subject me to administrative action (such as termination of employment or contract), civil penalties, and/or criminal penalties.

I agree and commit that if I hear, see, or otherwise become aware of actual or potential misuse of CJI, or of a situation that may cause or contribute to the misuse of CJI, I will promptly report same to Capt. Christopher Franks, Service Division.

I agree and commit that I will not allow, by action or inaction, the unescorted entry into any secure (protected) area by anyone who is not known to me to be authorized to enter such area.

I have read and understand the information above regarding the importance of protecting CJI, and have asked and received a satisfactory answer to any questions I had concerning the duties and restrictions imposed on me with respect to CJI.

_____ _____

Signature of Individual Date

_____

Company Employing the Individual

I hereby confirm that the above signed individual has read the above document (or had it read to him or her), and has been given the opportunity to ask questions. I have answered any questions and/or clarified any issues he or she posed regarding information security requirements.

_____ _____

Signature of Criminal Justice Agency Representative Date

KDPS MI 3949900

Criminal Justice Agency ORI