

ATTACHMENT A

SECURE CJIS FACILITIES ADDENDUM

SECURE CJIS FACILITIES ADDENDUM

Physical and logical access to secure facilities

I. Background

The FBI Criminal Justice Information Services (hereinafter referred to as "CJIS") Security Policy Version 5.6 mandates all agencies connected to the FBI CJIS systems adhere to regulation set forth within the CJIS Security Policy (hereinafter referred to as CSP). Part of the Security Policy outlines directives dealing with personnel security. Included within the term "personnel" are all individuals who are utilized by criminal justice agencies to implement, deploy, and/or maintain the computers and/or networks of the criminal justice agency which are used to access FBI CJIS systems. These individuals include city/County IT personnel, and private contractors.

The subject of non-criminal justice governmental personnel and private contractors is addressed in Sections 5.1.1.4 of the CJIS Security Policy and in the Security Addendum, which can be found in Appendix H. These sections include information on documentation which should be maintained in order to remain in compliance with the Security Policy.

II. Purpose

This Addendum establishes procedures and policies that will guide the parties to comply and adhere to the CJIS Security Policy pertaining to non-governmental personnel and private contractors.

These procedures will include the incorporation of the latest Security Addendums, fingerprint based background check, and the appropriate level of Security Awareness Training.

III. Background Checks

It may at times be necessary for contracted personnel to have unescorted access to judicial offices and other area containing certain criminal justice records/information. Before access is allowed, contracted personnel must complete a fingerprint passed back ground check as stated in CSP.

An authorization and consent for criminal background check form will be provided by the Sheriff/County. All contracted personnel who will provide the services herein described are required to complete, sign and return the authorization form. By signing the authorization and consent for release of personal information form, the contractor's personnel acknowledge that Sarasota County Government and the Sarasota County Sheriff's Office may conduct an investigation of criminal history information on file in local, state and national databases. The contractor shall forward the completed forms to Sarasota County Sheriff's Office Local Agency Security Officer (LASO) to perform the background checks for acceptance or rejection.

ATTACHMENT A SECURE CJIS FACILITIES ADDENDUM

IV. Approval and replacement of personnel

The Sheriff/County shall have the right to approve all contractor personnel assigned to provide services to secure CJIS facilities. Prior to providing services, the contractor shall provide at least 10 days written notice of the names and qualifications of the contractor personnel assigned to perform the services pursuant to the agreement. The contractor and any subcontractor being used by the contractor will be required to comply with the Criminal Justice Information Security Policy (CSP).

The Sheriff/County, on a reasonable basis, shall have the right to require the removal or replacement of any of the contracted personnel performing services, at any time during the term of the agreement. The Sheriff/County will notify the contractor in writing in the event the Sheriff/County requires such action. The contractor shall accomplish removal within forty-eight (48) hours after receipt of the notice from the Sheriff/County and shall promptly and within a time frame agreed by both parties replace such person with another person, acceptable to the Sheriff/County. The Sheriff's Office LASO and/or County shall be notified as soon as possible if any contracted employee is no longer employed by the contractor or providing further service to the Sheriff/County.

V. Remote access

Any contractor requiring remote access will be provided with administrative level unique log-in credentials to all servers, networks, databases and work stations that will be involved in the specific project. The remote connection will be secured via an approved FIPS 140-2 encrypted method. Contractors/vendors shall not disclose to any third parties any information contained in the Sheriff/County servers, networks, databases and workstations and shall not disclose any information to other employees of the contractor unless directly related to the services provided.