Community-Based Care
Information System Requirements

The department maintains information in the Florida Safe Families Network (FSFN) Information System (State Automated Child Welfare Information System (SACWIS) for the state of Florida). The department also maintains access to the Vital Statistics system to identify and verify data for children and parents when information regarding names, dates of birth, the place of birth or other pertinent addresses is received from the abuse hotline or other lawful sources. The provider must enter data into, and retrieve data from, these applicable systems. In accordance with Florida Statutes, Florida Administrative Code and departmental standards and procedures, the provider shall be required to exercise due diligence to ensure and maintain the accuracy, timeliness, and appropriate levels of security of information entered into, or retrieved from, these systems. It is expressly understood that the provider's violation of Ch. 119, F.S. or any associated Florida Administrative Code and departmental standards and procedures, may constitute sufficient grounds for a determination that the contract has been breached.

A. Security

1. The provider shall comply with all applicable laws and procedures pertaining to security and confidentiality including, but not limited to, those listed in the Community-Based Care Authority and Requirements Reference Guide.
2. The provider's own systems and premises shall be subject to inspection by the department's representatives at any time to verify compliance with security requirements.
3. Any data communications involving the department may also be monitored by department security or systems personnel for compliance with these requirements or misuse of the systems.
4. In the event that the provider is allowed to electronically connect to any of the department's facilities, the department may suspend or revoke that connection at any time without notice if the department has reason to believe that the security of the department's systems may be compromised by a continuation of that connection.
5. In the event the provider purchases, develops or maintains its own electronic information systems to support services provided through this contract, the department must have access to all information necessary to audit and examine such information in its native format, using access devices (terminals, personal computers, or other devices required) made available for this purpose by the provider. The provider must provide the department's representatives with the necessary system user accounts and passwords to access all information related to this contract which may be stored in the provider's systems.
6. The department may require the provider to accurately complete a self-audit questionnaire relating to the electronic information systems the provider and any subcontractors or affiliates participating under this contract use.
7. Material security violations or improper information disclosures shall constitute sufficient grounds for a determination that the contract has been breached.
8. At least annually, the provider will provide a listing to the department that includes, at a minimum, the name and user IDs of all users with access to above systems. Within 10 days of receipt of this listing, the department must certify to the provider Contract Manager that all user IDs listed are currently active and necessary. Any provider user IDs are to be defined as to whom they are for and the reason for the access. . During the term of the contract, the provider must also notify the department's Information Security Officer when any staff with access to mentioned systems is no longer employed for any reason. This notification must be provided within 2 business days of the separation.

9. The following summary of key security standards are applicable to all data covered by federal or state laws or regulations (Covered Data). The following list is not intended to be, and is not, exhaustive. The provider must comply with all security requirements related to Covered Data and any other State of Florida data provided to, or collected by, the provider acting on behalf of the department as its contractor. Further, the provider's employees, subcontractors, agents, or other affiliated third party persons or entities, as well as contracted third parties, must meet the same requirements of the provider under this contract and all agreements with the provider's employees, subcontractors, agents, contractors or other affiliated persons or entities shall incorporate the terms and conditions of data security into any contractual relationships established.

a. Access Controls:

(1) Viewing and modification of Covered Data must be restricted to authorized individuals as need for business related use.

(2) Unique authorization is required for each person permitted access to Covered Data and access must be properly authenticated and recorded for audit purposes, including HIPAA audit requirements.

(3) Access to all Covered Data provided to the provider's employees, subcontractors, contractors, agents, or other affiliated persons or entities must meet the same requirements of the provider under this contract and all agreements with same shall incorporate the terms and conditions of data security in the access authorization.

b. Copying/Printing (applies to both paper and electronic forms):

(1) Covered Data should only be printed when there is a legitimate need.

(2) Copies must be limited to individuals authorized to access the Covered Data and have a signed CF114 on file with the department.

(3) Covered Data must not be left unattended.

c. Network Security:

(1) All electronic communication including, but not limited to, Covered Data between the provider and the department shall use compatible, industry standard File Transfer Protocol software, using data encryption or a Virtual Private Network connection to ensure a secure file transfer at no additional cost to the department.

(2) Covered Data must be protected with a network firewall using “default deny” ruleset required.

(3) Servers hosting the Covered Data cannot be visible to the entire Internet, nor to unprotected subnets.

d. Physical Security (Servers, laptops and remote devices on which Covered Data is stored) (For purposes of these standards, mobile devices must be interpreted broadly to incorporate current and future devices which may contain or collect Covered Data.):

(1) The computing device must be locked or logged out when unattended.

(2) Servers must be hosted in a secure data center hardened according to relevant security standards, industry best practices and department security policies.

(3) Physical access to servers containing Covered Data must ensure physical access is monitored, logged and limited to authorized individuals 24X7.

(4) Routine back of Covered Data is required and backed up Covered Data must be stored in a secure off-site location.

e. Remote access to systems hosting Covered Data:

(1) Remote access to Covered Data must be restricted to the local network or a secure virtual private network.

(2) Unsupervised remote access to Covered Data by third parties is not allowed.

(3) Access to Covered Data by all third parties must adhere to the requirements of this contract.

f. Data Storage:

(1) Storage of Covered Data on a secure server in a secure data center according to relevant security standards, industry best practices and department security policies is required.

(2) Covered Data stored on individual workstations or mobile devices must use whole disk encryption. Encryption of backup media is similarly required to be encrypted.

(3) Covered Data is not to be transmitted through e-mail or social networking sites unless encrypted and secured with a digital signature.

10. The provider must meet all of the department and State requirements for individual employee security, information security, and physical security of all non-public data in the possession of the provider.

11. The provider acknowledges that all Covered Data, other data and department content uploaded to the provider's servers, workstations or mobile devices from the department, or made accessible to the provider's servers, workstations or mobile devices or personnel remains the property of the department.

12. Termination provisions related to Data:

Within 30 days after the termination or expiration of this contract for any reason, the provider shall either: return or physically or electronically destroy, as applicable, all Covered Data provided to the provider by the department, including all Covered Data provided to the provider's employees, subcontractors, agents, or other affiliated persons or entities according to the standards enumerated in D.O.D. 5015.2; or in the event that returning or destroying the Covered Data is not feasible, provide notification of the conditions that make return or destruction not

feasible, in which case, the provider must continue to protect all Covered Data that it retains and agree to limit further uses and disclosures of such Covered Data to those purposes that make the return or destruction not feasible as the provider maintains such Covered Data. This includes any and all copies of the data such as backup copies created at any provider site. Upon request by the department, made before or within sixty (60) days after the effective date of termination, the provider will make available to the department for a complete and secure (i.e. encrypted and appropriated authenticated) download file of department Covered Data in XML format including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. The downloaded file shall include all Covered Data provided to the provider's employees, subcontractors, agents, or other affiliated persons or entities must also comply with this requirement. The provider's employees, subcontractors, agents, or other affiliated persons or entities must be available throughout this period to answer questions about data schema, transformations, and other elements required to fully understand and utilize the department's data file.

B. Liability for System Failure

1. The department is not liable to the provider for a failure of any of the department's systems or for the degradation or disruption of any connection or system. Provider loss or diminution of access to the department's systems for any reason shall not excuse the provider from its obligations under this contract.

2. The provider shall be held accountable for late data input due to a department systems failure of less than one working day. Department systems failure of more than one working day shall be calculated as follows: For each additional working day of department systems failure, the provider shall have two working days for data input before they are held accountable for late data input.

C. Integrated Child Welfare Service Information System

1. ICWSIS is currently the department's system of records for child-specific expenditures and is the source of the OCA Summary Report submitted with the provider's invoice. The provider shall enter data into ICWSIS, or to the FSFN system at any time when the department determines that FSFN has subsumed ICWSIS, within 48 hours to indicate changes in a child's living arrangements or legal status or changes made to a foster home's status. The provider specifically agrees that ICWSIS and FSFN will always contain the most current and the most accurate information regardless of any other systems employed by the provider.

2. The provider specifically agrees to collect, enter and maintain all data to meet ICWSIS and FSFN requirements in accordance with the department's policies and procedures, including timeliness criteria.

D. Vital Statistics

1. The Vital Statistics Birth Registration System maintains official records of births within the state, as well as births to Florida residents which occur out of state. Authorized users have on-line access to birth records to identify and verify data for children and parents when information regarding names, dates of birth, place of birth or addresses is received from the abuse hotline or other lawful sources.

2. The provider shall comply with the current Memorandum of Understanding (MOU) between the department and the Department of Health (DOH), which sets the parameters for access to the Vital Statistics system by the Family Safety Program and its agents.

E. Florida Safe Families Network (FSFN) Requirements

Florida Safe Families Network is the department's system of record for all child welfare casework. The provider specifically agrees that Florida Safe Families Network will always contain the most current and the

most accurate information regardless of any other systems employed by the provider.

1. The provider shall collect, enter and maintain all data to meet Florida Safe Families Network system's requirements in accordance with federal requirements and department policies and procedures, including timeliness criteria.

2. Caseworkers shall be responsible for verifying on a regular basis, and no less than monthly, the accuracy and completeness of all data relating to their assigned cases within Florida Safe Families Network.

3. The provider is responsible for purification of data for the geographic area served by the provider in State systems that may be necessary before any future automated conversion of data from current systems to Florida Safe Families Network.

   a. This includes data entered before the provider assumed responsibility for services.

   b. The provider is also responsible for any manual data conversion activities required.

   c. If additional funds are made available to the Region for this purpose, a proportionate amount may be added to this contract for a similar level of effort.

4. Joint Application Development (JAD) Sessions and User Acceptance Testing;

   a. The provider shall participate in JAD sessions and user acceptance testing during the development and operation of Florida Safe Families Network.

   b. The provider shall be responsible for any travel costs associated with attendance at these sessions.

5. Application Training.

   a. The provider shall participate in application training for use of Florida Safe Families Network as required during the deployment of future Florida Safe Families Network functionality.

   b. The provider shall be responsible for any travel costs associated with attendance at these training sessions.

6. Site Survey.

   a. The provider agrees to allow the department to conduct a site survey to determine needs related to the implementation of Florida Safe Families Network at the provider's site(s).

   b. The department agrees to determine the resources needed to equip the provider's staff and in evaluating site security requirements.

7. Equipment.

   a. The provider shall not use equipment provided by the department and purchased with Florida Safe Families Network system's funds for any purpose other than to support staff providing Title IV-E and IV-B eligible services in accordance with the department's federally approved cost allocation plan for Florida Safe Families Network.

   b. Florida Safe Families Network computer equipment shall not be transferred, replaced or disposed of by the provider without prior permission of the department's contract manager.

8. The provider shall not have access to State owned applications, e.g., FSFN, ICWSIS, etc., to resolve data issues requiring direct database access, make software changes, add programming, etc. The provider shall be responsible for, with appropriate access authorization to the State owned application, maintaining data and resolving data issues through direct on-line access and/or requests to the department for direct database changes.

F. Information Technology (IT) Modernization

Information Technology Modernization includes the purchase of planned or directed changes in technical sophistication application systems and equipment.

1. The provider may purchase new or replacement IT in accordance with policy and procedures listed in the Community-Based Care Authority and Requirements Reference Guide.
2. Replacement of department furnished IT necessary in the performance of this contract shall be procured by the provider and funded against payments made under this contract at no additional cost to the department.
3. The provider shall provide new or factory reconditioned parts and components when practicable in providing maintenance and repair services as described herein.
    a. All replacement units, parts, components and materials to be used in the maintenance and repair of equipment shall be compatible with existing equipment on which it is to be used and shall meet industry standards and be suitable for their intended use.
    b. If material that meets the accepted industry standard cannot be obtained, the provider must obtain the concurrence of the Region's Information Systems Director before using alternate materials.

G. Data Analytics

The department intends to establish guidelines and requirements that incorporate data analytics in improving service delivery to clients. Data analytics is the process of examining raw data with the purpose of drawing inferences or conclusions from that data. Data analytics should be used to allow case workers to make better business decisions for client services. Data analytics may involve the process of sorting through huge data sets using sophisticated software to identify undiscovered patterns and establish hidden relationships. The department may also deliver or require the use of applications performing data analytics. The provider shall update quarterly, annually, and biannually the data analytic system(s) as directed by the department, depending on the analytic and relevant cycle time for updates. The data analytic system(s) may report outcomes through one or more dashboards which should allow users to drill down for more granular information for that particular analytic.

H. Information Technology Support

The purpose of this section is to define the areas of IT support and responsibility between the provider and the department's Region Management Information Systems. Certain conditions based on physical location of the provider staff, department staff, ownership of the building leases and ownership of the facility Local Area Network (LAN) and Wide Area Networks (WAN) connections will impact the specific IT support for the provider.

1. The provider, not the department, shall be responsible for their own networks and network applications, including, but not limited to, e-mail, network operating systems, MS Windows, MS Word and other like applications.
2. The provider shall maintain a support center for their staff to call before any contact is made with the department's Customer Assistance Center, and the provider's support center will make a determination if the issue is related to a State owned application. State owned applications shall be defined as any application developed and maintained by the department.
3. LAN issues shall be the provider's responsibility. The provider's LANs and the software supporting those LANs are not State owned applications or LANs until the provider transfers the original equipment or equipment they purchased during the term of the contract back to the department to

replace the original equipment.

4. WAN issues shall be the provider's responsibility from the provider's PC to the network point of presence that connects the provider to the WAN.

5. The department or the State shall be responsible from the WAN point of presence to the department's central data processing facility.

H.1. With respect to IT support for provider staff located in a department facility, where the LAN and WAN connections are controlled by the department, the following will be supported:

1. In the case of trouble or suspected trouble requiring the assistance of department personnel, the provider will call the department's Office of Information Systems Customer Assistance Center in Tallahassee.

2. The Customer Assistance Center will be the initial contact point for support and to request assistance. The provider staff will identify such calls as fault calls, so that the appropriate level of urgency can be applied.

3. All IT support will be documented by means of a generated work order by the department.

4. The provider acknowledges that abuse of this technical support facility would lead to degradation in service to other providers and department users.

5. The department reserves the right to charge for Customer Assistance Center calls that are caused by failure of provider-owned equipment outside that approved by the department or incorrect operation of the provider's equipment.

6. The department will make reasonable efforts to maintain constant access to the State's network and ensure that the network is available for use by the provider.

7. The department shall not be held responsible for non-availability or outages of service, or for unforeseen interruptions to service.

8. The department shall not be held responsible for any loss or damage incurred by the provider or any other person caused by any failure of any nature on the part of third party service suppliers, to supply the provider with sufficient services and connections, to maintain the quality of service or network that the department may be endeavoring to supply.

   a. Services to be provided include:

      1) Network Support of Core Service Switches and Routers

      2) Support of Core Service Firewalls

      3) Support of Network Management hardware and software

      4) Support of Dynamic Host Configuration Protocol (DHCP) services

      5) Support of Domain Name Server (DNS) services Connectivity to the internet

      6) Support of Simple Mail Transport Protocol (SMTP) gateway e-mail services

      7) Review/Replacement of core service network

      8) Provide premise wiring installation and maintenance

   b. Other Services:

      1) Network design and architecture

      2) Network capacity planning

3) Support of wireless networking

4) Wireless design

5) Network change management and problem management

6) Support and hosting of Network servers and associated equipment within a department-owned computer room.

9. Hours of Service Availability for access to Network Support Service available Monday – Friday, from 7:00 a.m. – 5:00 p.m. excluding State holidays. Network monitoring will be staffed twenty-four (24) hours per day Monday – Saturday.

10. Department staff will evaluate, engineer, purchase, configure, install, troubleshoot and maintain the backbone data network switches, servers, and software as deemed appropriate by the Region Information Systems Director.

11. Department staff will troubleshoot all LAN/WAN connections. If any LAN connection requires repair or replacement, then it is the responsibility of the department to pay for these repairs or replacements. The Region Information Systems Director will be responsible for bringing in outside hardware vendors when necessary to repair or replace defective or nonfunctional components, where cost effective. Replacements will be made with "like" equipment. The department agrees to coordinate with the provider staff to resolve WAN access to any required State application(s).

12. Any new data wiring required by the provider for connectivity in DCF facilities must be approved by the department, through the Information Resource Request (IRR) process, and all associate wiring costs shall be paid by the provider.

13. Department personnel will assume responsibility for keeping network operating systems updated with current patches and revisions and to install and configure appropriate device access to any required State application(s).

14. The department shall provide network security for State-owned applications. The provider shall provide PC software and network security software products and access assistance to provider staff for non State-owned applications. Example: Seagull Corporation's BlueZone software.

15. Any installation of any type of provider Network Server on a department-owned LAN must be approved by the department's Region Information Systems Director.

H.2. With respect to IT support for provider staff located in a provider facility where the LAN and WAN connections are controlled by the provider, the following will be supported:

1. The department agrees to coordinate with the provider staff in the installation, configuration and security access to any state owned application(s).

2. The department agrees to install and configure appropriate device access to any required state application(s).

3. The department agrees to coordinate with the provider staff to resolve WAN access to any required state application(s).

4. Provider staff may optionally call the Customer Assistance Center in Tallahassee for first line of support, or they can call their own provider network helpdesk support first. If the provider's staff calls the Customer Assistance Center, the provider staff will identify such calls as fault calls, so that the appropriate level of urgency can be applied. All such IT support will be documented by means of a generated work order by the department.

5. The provider acknowledges that abuse of this technical support facility would lead to degradation in service to other

provider's and department users.

6. The department reserves the right to charge for Customer Assistance Center calls that are caused by failure of provider-owned equipment outside that approved by the department or incorrect operation of the provider's equipment.

7. Provider staff will troubleshoot all LAN/WAN connections. If any LAN connection requires repair or replacement then it is the responsibility of the provider to pay for these repairs or replacements.

8. Any new data wiring required by the provider for connectivity must be approved by the department's Region Information Systems Director, through the IRR process, and shall be paid by the provider.

9. The department shall provide network security for State-owned applications.

10. The provider shall provide PC software and network security software products and access assistance to provider staff for non State-owned applications. Example: Seagull Corporation's BlueZone software.

11. The provider shall provide network security software products and access assistance to the provider staff for all applications.