Terms and Conditions
For Access to OCFS Data

Parties:

The parties to this "Terms and Conditions" are the New York State Office of Children and Family Services, with principal offices at 52 Washington Street, Rensselaer, New York 12144 ("OCFS") and **[Requesting Entity]** _____with principal offices at _____("Requestor".)

1. Purpose

The "Terms and Conditions" set forth below inform the Requestor of the terms, conditions and requirements for access to and the appropriate handling of personal and confidential client identifiable information stored, accessed or obtained from OCFS' **[insert data source]** by Requestor's employees, contractors, employees of such contractors, volunteers and any other person authorized by Requestor to access the **[data source].** These "Terms and Conditions" are applicable to all of Requestor's organizations, branches, contractors or subcontractors and/or individuals in any geographic region who are permitted to have access to any data that originates or resides in OCFS' systems or applications. The Requestor may impose more stringent standards than those required herein.

These Terms and Conditions for Access to OCFS' **[data source**] must be signed by the Requestor's Commissioner, Executive Director, President, or Chief Executive Officer, as appropriate, and received and approved by OCFS and OCFS' designated representative of the New York State Office of Information Technology Services ("ITS") prior to any information being disclosed from OCFS' **[data source].**

2. Legal and Regulatory References

Access to, retention, re-disclosure and destruction of the information contained in OCFS' **[data source]** are subject to applicable federal and state statutory, regulatory and policy requirements, including but not limited to those listed in Attachment A, which is incorporated and made part of the Terms and Conditions. Additional confidentiality and privacy requirements related to other state and federal entities and systems may also apply. The signing of this document by Requestor's Commissioner, Executive Director, President, or Chief Executive Officer, as appropriate, signifies agreement with all terms and conditions of this document, including those relating to record access, confidentiality, disclosure, retention and destruction or disposal of records.

3. Purpose and Scope

Requestor is granted access to OCFS' **[data source]** for only those purposes and for so long as set forth in the attached "Application for Access to Confidential OCFS Information" annexed hereto as Attachment B and incorporated herein.

OCFS' **[data source]** will provide a data feed to the Requestor of only that data to which the Requestor is authorized to access in the CONNECTIONS application or any other application(s) pursuant to these Terms and Conditions. No progress notes will be included in the data transmitted from OCFS' **[data source]**.

These "Terms and Conditions" applies (but is not limited) to the handling, protection, security and non-disclosure of all confidential information, including client identifiable information, data or systems originating or residing in OCFS' **[data source]**. Access to OCFS' **[data source]** and the information contained therein must only be granted on a "need to know" basis. Only when it has been determined by Requestor that a particular individual's job duties require access, and all agency permissions, requirements and laws and regulations have been satisfied, may the individual be granted access to OCFS' **[data source]**. Access to OCFS' data or information shall only be permitted to the extent and for the duration necessary to perform the required services. Access must be terminated in accordance with Attachment B herein, when the "need to know" no longer exists for that individual or the duration specified in the "Application for Access to OCFS Information" has expired.

4. **Individual/Employee Access**

Before any individual or employee is given access to any OCFS data by Requestor, that individual/employee must sign the "OCFS Non-Disclosure Agreement", Attachment C herein. The signed Non- Disclosure Agreement (Agreement) must be sent to OCFS' designated representative of ITS prior to any individual/employee being permitted access to any OCFS data. Copies of signed Non-Disclosure Agreements must be maintained by the Requestor for a period of six (6) years following the employee/individual's last known access to the OCFS data.

Except as specifically authorized by Requestor, no individual/employee shall be authorized at any time, in any fashion, form, or manner, either directly or indirectly, to divulge, disclose, communicate or use, either prior to, during or subsequent to any engagement, any confidential information or methods of accessing information or data received, obtained, acquired, directly, indirectly or accidentally, or developed in association with any engagement or employment.

All confidential or proprietary information obtained or accessed from OCFS' **[data source]** in accordance with these Terms and Conditions is and shall at all times remain the property of OCFS. Requestor will destroy all reports, notes, memoranda, notebooks, drawings, and other information or data accessed, developed, received, compiled by or delivered to Requestor and/or individual/employee relating to any engagement for services, regardless of the source of said information, upon termination of any engagement, employment or Need-to-Know. Destruction includes the complete

purging of all confidential information from all computers and back up media storage in a manner to protect confidentiality. Upon completion, the Requestor must certify to OCFS in writing that it has complied with the obligations set forth in this section.

Requestor, its employees and agents will use only those access rights and shall access only those directories, information or data authorized by OCFS. All requests for access must be communicated to OCFS' Systems Administrator, and OCFS' designated representative of ITS. The consent of OCFS' designated representative of ITS shall be required with respect to any access to OCFS data.

Requestor agrees that any and all OCFS data accessed pursuant to this Agreement shall be transmitted through the use of secure methods as designated and approved by OCFS and ITS for such purposes.

Any hard copy of OCFS data must be stored in secure, locked containers. Where data is stored on a computer or any other storage media, including but not limited to removable drives or CD ROMs, the Requestor must have an appropriate computer security policy, approved by OCFS' designated representative of ITS that protects confidential information from unauthorized access and disclosure. The computer security policy must include provisions that address the physical security of computer resources; equipment security to protect equipment from theft and unauthorized use; software and data security; and access control. Any access to the stored data, wherever stored, must be limited to Requestor's employees, volunteers and other staff that have signed the Non-Disclosure Agreement. Responsibility for computer security must be assigned to a named individual or employee of Requestor and that assignment must be documented in the security policy.

Requestor must familiarize all individuals/employees with authorized access to the requested data with the applicable security policy requirements before access is granted to such individual or employee.

Requestor agrees that if it breaches, or threatens to breach any of these Terms and Conditions, OCFS shall have a right to immediately terminate any access granted pursuant to these Terms and Conditions. Additionally, OCFS shall have all equitable and legal rights (including the right to obtain injunctive relief) to prevent such breach and/or to be fully compensated (including reasonable attorneys' fees) for losses or damages resulting from such breach. Requestor acknowledges that compensation for damages may not be sufficient and that injunctive relief to prevent or limit any breach of confidentiality may be the only viable remedy to fully protect the confidential or proprietary information accessed or obtained pursuant to these Terms and Conditions.

Notwithstanding the provisions of Section 208 of the State Technology Law or Section 899-aa of the General Business Law, in the event of a breach of any and all data or information received pursuant to these Terms and Conditions, Requestor shall be responsible for complying with any and all notifications and other required actions pursuant to State Technology Law Section 208 and/or General Business Law Section

899-aa, together with all costs attendant to such notices.. Requestor shall provide OCFS with a copy of its Breach Notification policy/protocol, and verify that its employees and agents are aware of its obligations regarding such a Data Breach. In the event of such a breach, Requestor shall immediately notify OCFS of the breach, and also commence an investigation as to the scope of the breach, and take any and all steps to restore security to Requestor's system. Requestor must first consult with OCFS prior to notifying any individual whose data or personal information has been breached, and prior to informing the Consumer Protection Board, the Attorney General's Office, the NYS Office of Information Technology Services, any consumer protection agencies, or the New York State Police.

Upon request, Requestor must provide State or federal auditors with access to relevant records or documentation of compliance with these Terms and Conditions, the Non-Disclosure Agreements and applicable laws and regulations. At the discretion of OCFS or any other authorized federal or State entity, a site visit may be conducted to audit compliance with these Terms and Conditions, the Non-Disclosure Agreements, and applicable laws and regulations.

5. **Reporting Problems**

What To Report: Requestor, Requestor's employees, contractors, subcontractors, volunteers or any individual, including but not limited to third parties, contractors, consultants, temporary employees, researchers and other workers must immediately report any compromises or suspected compromises of State data or information systems, or the unauthorized disclosure of confidential information to:

By Email:
acceptable.use@ocfs.ny.gov

6. **Duration of Access/Renewal**

Access to OCFS data as set forth herein and in the "Application for Access to Confidential OCFS Information" shall be for the shorter of the time period specified in the "Application" or when Requestor no longer has a Need-to-Know with respect to access to the data, whichever occurs first. Where Requestor desires continued access to the OCFS data beyond the date specified in the Application, a written request must be submitted and approved by OCFS and ITS.

Nothing herein shall affect OCFS' right to terminate access to the requested data without notice.

Further Information: For questions about this document, or copies of the Non Disclosure Agreements, please contact the OCFS Information Security Officer at the following address:

OCFS Information Security Officer
52 Washington Street, 309S
Rensselaer, NY 12144

Signed:

Commissioner/Executive Director: _____

Requestor Name _____

Attachment A

Legal and Regulatory References

This policy addresses compliance with, and incorporates a variety of federal and state legal, regulatory and policy requirements, including the following:

- Child Abuse Prevention and Treatment Act (CAPTA), as amended (42 U.S.C. 5101 et seq.) - section 106
- Statewide Automated Child Welfare Information Systems (SACWIS)
- Federal Regulation 45 CFR 95.621; 45 CFR 205.50; and 45 CFR 1355.21 (a)
- New York State Executive Law § 501-C;
- New York State Social Services Law §§ 372, 422, 422-a, 424-a, 444, 459-g and 473-e;
- New York State Public Health Law Article 27-F;
-New York State Mental Hygiene Law §§ 33.13 and 33.16;
- 9 NYCRR 164.7 and 168.7;

- 18 NYCRR §§ 339, 346.1(e), 347.19, 357, 357.3, 358-5.8, 358-5.11(b), 387.2 (j), 423.7, 431.7, 432.7, 452.10, 457.16 465.1 and 466.4;
- Social Services Law, Section 136;
- Social Service Law Article 2, Section 23;
- Social Services Law Article 3 Title 6-B and Section 111-v;
- Social Security Act, Title IV, Sec. 1902(a)(7);
- State TANF Plan, Sec. A (iii) & Appendix B (18 NYCRR 357);
- 7 USC 2018(c), 2020(e)(8); 7 CFR 272.1(c);
-42 CFR Part 2 (Confidentiality of Alcohol/Drug Abuse Records)
- 42 CFR 431.300 – 306;
- 45 CFR 302.35(c); 303.21(a); 307.13(a);
- 45 CFR Chapter II, Part 205, Sec. 205.5;
- 42 USCA 653(a)(h); 653(b)(2); 653 (c); 654a(d),(c); 654(26); 654(26)(e); 663(d); 666(a)(17); 666(c)(1)(D); 669a(b) and 671(a)(8);
- 42 USCA Sec. 1320(b)-7;
- IRS Publication 1075; IRC 86 at 103(L)(8); 226 USCA 6103(L)(8);

- Tax Law 1825;
- Family Educational Rights and Privacy Act (FERPA), as amended (20 USCA § 1232g; 34 CFR Part 99);

- Driver's Privacy Protection Act (DPPA) Public Law No. 103-322 codified as amended by Public Law 106-69;
- Electronic Signatures and Records Act (ESRA) New York State Consolidated Laws State Technology Law, Article I;
- Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Internet Security and Privacy Act NYS Technology Law, § 203; NYS Executive Order 117; NYS Executive Law 206-a;
- Public Officers Law Personal Privacy Protection Law, Article 6-A;
- Penal Law, § 203 Article 156 Offenses Involving Computers; Definition Of Terms;

10 7/11/05 Appendix 5 - I/EDR RFP Local Commissioners Memorandum 04-CIO-”Terms and Conditions”-01 I/EDR RFP Local Commissioners Memorandum

- Freedom of Information Act (FOIL) Public Officers Law, Article 6, Sections 84-90;

- State archives and records administration (SARA) Arts and Cultural Affairs Law (ACAL), §57.05; §57.25

- NYS Office of Cyber Security and Critical Infrastructure Coordination Information Security Policy P03-002;
- NYS Office of Cyber Security and Critical Infrastructure Coordination Incident Reporting Policy P03-001;
- NYS Office of Technology Policy P2003-001 Customer Use and Access of the Human Services Enterprise Network;
- NYS Office of Technology Policy P03-001 Directory Services – Directory Account Management;

- NYS Office of Technology Customer Networking Solutions Standard S2003-001 Data Storage Sanitization;

- Medicaid Privacy Regulation §1902(a)(7) of the Social Security Act (42 USC §1396a(a)(7))as implemented in regulations at 42 CFR §431.300 et seq. 42 CFR §431.302

- Health Insurance Portability and Accountability Act (HIPAA) pertaining to the Confidentiality and security of MCD/PHI/ at 42 USC Chapter 7, Subchapter XI, Part C; 45 CFR Parts 160 and 164
- Section 537 of the Labor Law and 42 USC 1320b-7, 42 USC 503, and 20 CFR Part 603
-