	Tennessee Department of Children's Services **Protocol for DCS Electronic Record System Management, Data Requests, and Data Corrections**
	Supplemental to DCS Policy: *7.5, Information Technology Requests*

A. Glossary

1. Department of Children's Services (DCS) HR (Human Resources): The Human Resources designee is the HR representative who processes a new employee and/or employee separation from DCS.

2. Edison: A main database the State of Tennessee uses that maintains state employee information and state-related functions.

3. Strategic Technology Solutions (STS): Strategic Technology Solutions is a division within the Department of Finance & Administration (F&A) that provides planning, resources, execution, and coordination in managing the information system needs of the State of Tennessee.

4. STS Access Management: A team within Strategic Technology Solutions (STS) who creates, monitors, and disables state network access for state employees and non-state employees.

5. STS Field Customer Care Representative (FCCR): Field Customer Care Representatives are specialized STS staff who perform customer care duties and establish various access to programs within the state network for state employees and non-state employees.

6. ServiceNow (SNOW): Internal form submitted via a direct link requesting a change in user account access that routes automatically to STS.

7. Private Provider: Any outside organization contracted with DCS to provide services to children and families.

8. DCS Electronic Record System: A DCS owned Information Technology System utilized for all data entry, collection, and documentation associated with children and family cases.

9. Comprehensive Child Welfare Information System (CCWIS): The Comprehensive Child Welfare Information System is the Electronic Record System used for case management.

10. Office of Data Governance and Analytics (ODGA): The Office of Data Governance and Analytics (ODGA) is the division within DCS that governs compliance of data for the integrity of its collection, usage, and storage.

11. Data Correction, Issue, or Modification Requests: Any request to change data entry, in which the DCS employee isn't authorized to change, in the Electronic Record System. Data issues, corrections, or modification requests also include data not displaying correctly in a report and/or not in accordance with current policy for data integrity.

B. DCS Electronic Record System Access Management and Data Related Requests

The ODGA receives and reviews all data issues, corrections, or modification requests, new report requests, and data extract requests. Upon approval, ODGA completes the request and/or partners with the appropriate parties for completion.

C. How to Submit a Data Issue, Data Correction, or Data Modification Request

1. All data issues, corrections, or modification requests are submitted to the Office of Data Governance and Analytics (ODGA) using the following link: **https://stateoftennessee-cvlyz.formstack.com/forms/data_issue_notification**.
2. Any data issue, correction, or modification request that involves the deleting of information from the DCS Electronic Record System (i.e. case recordings, adoption records, or other alterations of the original electronic case file) requires approval from a program Executive Director and Legal in the request.

   Note: Altering the Electronic Case Record may only be completed by authorized individuals with appropriate approval, as portions of the Electronic Record System may have been given to legal entities (i.e. courts/attorneys) and/or the child/family.
3. ODGA reviews all data issues, corrections, or modification requests, verifying required information is included, and routes to the correct parties (STS, Safe Measures, STS FCCR, etc.) for completion.
4. ODGA monitors the data issue, correction, or modification request until completed and confirmed with the requester.
5. Once the data issue, correction, or modification request is made, ODGA verifies the information is now correct with the requestor.
6. All data issues, corrections, or modification requests are maintained within ODGA.

D. How to Request New Reports or Data Extract Requests

1. New Report Requests:

a) Before submitting a new report request, the requestor should search **Reports Central** and **Safe Measures** to determine if a report already exists.

b) If a report does not exist, the requestor submits a new report request form through the following link: **https://stateoftennessee-cvlyz.formstack.com/forms/data_request_form**.

c) The ODGA Data Director reviews the new report request form and determines approval or denial.

d) If approved, ODGA works with appropriate parties and the requestor to facilitate the new report request.

e) ODGA monitors the new report request until completed.

f) ODGA confirms with the requestor that the new report meets the needs prior to completion of the request.

g) All new report requests are maintained within ODGA.

2. Data Extract Requests:

a) Data that is not available in currently produced reports and/or not available in systems of which the requestor has access can be requested as a one-time data extract by filling out and submitting a request through the following link: **https://stateoftennessee-cvlyz.formstack.com/forms/data_request_form**.

b) Once the request has been submitted, the Data Analytics Director/designee will contact the requestor to review the data extract request and prioritize the request if it is approved. **If the data will be reused or needed more than one time, a new report request should be considered (see #2 request type above).

c) A decision of approval or disapproval of the request is based on the following factors:

- Applicable State and Federal Rules and Laws or applicable accreditation standards.

- ♦ The purpose for which the information is to be used and benefits to DCS.
- ♦ Ability of DCS to provide the requested information.
- ♦ Cost (time and staff resources) of providing the requested information, including the frequency the data will need to be provided.
- ♦ Feasibility, merit, potential outcome, and benefit of the research project and/or results.

d) Please note, any requests originating from persons outside of DCS, or requests where the requested information will be shared with any person or entity outside of DCS (Community partner requests, non-profit requests, academic course work, etc.), are subject to additional review by the DCS Legal/Privacy Team and the requestor must provide DCS a legal and/or privacy point of contact.

e) All data requests are maintained within ODGA.

E. DCS Employee Access to the DCS Electronic Record System

1. Requesting New Employee Access:

a) DCS HR will have the new employee sign the Employee Code of Conduct upon initial hire and annually thereafter agreeing to acceptable usage.

b) DCS HR enters the required information into Edison for the new DCS employee, which automatically notifies STS of a new hire.

c) DCS HR also submits an Onboarding request, via Service Now (SNOW), and sends request to STS Access Management.

d) STS Access Management sets up an Active Directory (AD) account, which is required to access state network.

e) Once STS Access Management tasks are complete, the SNOW request is assigned to STS FCCR.

f) STS FCCR sets up the new DCS employee record in the Electronic Record System based on the information provided from Edison.

g) STS FCCR creates the new DCS employee record and applies security access, which governs what system modules, functions, and information the DCS employee can access. Security access is granted based on: Job Title and Program Area (Child Protective Services, Juvenile Justice, Foster Care, Child Abuse Hotline, etc.).

h) The Electronic Record System training for new DCS employees is completed in pre-service training and will be documented within pre-service records.

2. Requesting Changes in Access:

a) When a change in an employee's access is warranted, the DCS employee completes **CS-4287, Electronic Record System Request for DCS Employees** and submits it to their program director.

b) The program director reviews and approves the change in access request, verifying the change request is needed for the DCS employee's job duties, role, and/or program area and routes to the executive director for final approval.

c) The DCS employee or program director enters a SNOW request for the access change in the Electronic Record System with the approved **CS-4287, Electronic Record System Request for DCS Employees** form attached.

- **Create TFACTS Request - Children's Services Service Portal**

Note: STS FCCR will only implement a change in employee access with an approved **CS-4287, Electronic Record System Request for DCS Employees** attached, verifying all requirements are met, and the change is justified. E-mails requesting a change in access without a completed SNOW Electronic Record System request and approved **CS-4287, Electronic Record System Request for DCS Employees** will not be implemented.

d) STS FCCR terminates any current access no longer authorized based on the change in user's access request, as applicable.

- **Example**: If a change in access is a result of a program area change, access to modules no longer authorized is disabled when completing the request.

- A change from a program area with restricted module access (SIU, Adoptions, Restricted Family Case) is automatically disabled when processing the change in access request.

e) SNOW Electronic Record System requests and accompanying **CS-4287, Electronic Record System Request for DCS Employees** will be maintained/archived in SNOW.

f) When a change in employee's access results in new modules in the DCS Electronic Record System, the DCS employee completes Electronic Record System training for the newly granted modules.

- All employees can access the Electronic Record System training online or through the Office of Training and Professional Development. **https://www.tn.gov/dcs/for-providers/tfacts-and-training/tfacts-help-documents.html**.

g) DCS employees are required to notify their supervisor immediately if they discover they have access that should not be authorized or when a conflict of interest arises with their current access in the Electronic Record System.

h) A change in employee access that requests access to restricted cases and/or modules in the Electronic Record System requires additional approval from the program director and/or legal.

- Restricted cases may include, but are not limited to, restricted family case(s), Special Investigation Unit, and/or Adoption.

- Access to a restricted case is only authorized for that specific case; access to all restricted cases requires Executive Director approval.

- Any restricted case access request must include an end date noted on **CS-4287, Electronic Record System Request for DCS Employees**.

- STS FCCR notes the end date when granting the access to the restricted case and suspends the access on the end date.

- If additional access time is needed, a new **CS-4287, Electronic Record System Request for DCS Employees** must be submitted.

i) When an employee is on approved extended leave, HR submits a SNOW request to temporarily suspend Electronic Record System access for the duration of the approved leave.

3. Requesting Termination of Access to the DCS Electronic Record System:

a) On the same day of an employee's separation from the DCS, HR/designee submits an offboarding request through SNOW to terminate an employee's state network access to include the Electronic Record System.

b) STS FCCR receives the SNOW request and terminates the former DCS employee's access to the Electronic Record System within 24 (twenty-four) hours of receiving the form.

c) If the employee is terminated on the last day of the week, DCS HR should contact the STS FCCR directly, in addition to entering the SNOW request, to ensure the FCCR is aware and can terminate access to the Electronic Record System on the same day before the weekend starts. This is non-negotiable.

d) All SNOW Electronic Record System requests terminating a DCS employee's access will be maintained/archived in SNOW.

e) DCS staff account access will be suspended automatically after 60 (sixty) days of inactivity.

4. Audit of DCS Employee Access in the DCS Electronic Record System:

a) The Electronic Record System has a module entirely devoted to creating, updating, maintaining employee information, to include their Electronic Record System security. Security level(s) on this screen will align with the DCS employee's job title and work unit.

b) For DCS employees with additional access levels in the Electronic Record System, **CS-4287, Electronic Record System Request for DCS Employees** and SNOW Electronic Record System request will be on file validating the added access levels.

c) Quarterly, ODGA reviews DCS active employees with access to the Electronic Record System who haven't logged into the Electronic Record System in over 60 (sixty) calendar days, has restricted access, and/or upon request, for compliance.

d) ODGA works within the aforementioned request processes to resolve any errors in the Electronic Record System access levels.

e) The Electronic Record System runs a script nightly that automatically suspends any user's access if the user has not logged into the Electronic Record System for 60 (sixty) calendar days.

5. DCS Employee Access in Safe Measures:

a) Access in Safe Measures is only provided based on the employee's job responsibilities and program assignment.

b) When a new DCS employee needs new user access to Safe Measures, the employee contacts STS FCCR at **EI_DCS_FCC_Central Office@tn.gov** to request approved access.

c) When a current DCS employee needs a change in access in Safe Measures, the employee completes the data issue notification using the following link: **https://stateoftennessee-cvlyz.formstack.com/forms/data_issue_notification**.

d) ODGA reviews the change in access request and works with the employee and Safe Measures to complete the request.

F. Private Provider Employee Access to the DCS Electronic Record System

1. Requesting Access for a New Private Provider Employee:

a) When access to the DCS Electronic Record System is needed by a private provider (non-DCS) employee, they must complete the following steps:

- The private provider ensures all required personnel documentation, including background checks, is complete and on file PRIOR to requesting employee's access to the Electronic Record System in accordance with the Contract Provider Manual.
- The employee's supervisor and/or private provider designee completes the DCS Electronic Record System Access Request **CS-0944, Electronic Record System Access Request for Providers** form, only requesting access for the user to perform assigned job duties.
- The employee receiving access reviews and signs the Acceptable Use Policy Network Access Rights and Obligations.
- Both completed forms are e-mailed to: **EI-DCS.ProviderRelations@tn.gov** (which is now being monitored by ODGA).

b) Once completed forms are received, ODGA reviews and submits a provider onboarding request in SNOW for those warranting Electronic Record System access.

c) Request is assigned to STS Access Management Team.

d) STS Access Management Team sets up a non-state employee network account.

e) Once STS Access Management completes their tasks, the SNOW request is assigned to STS FCCR group.

f) STS FCCR sets up a new employee record in the Electronic System using the completed **CS-0944, Electronic Record System Access Request for Providers**, only granting the requested access level in the Electronic Record System.

g) Prior to the Electronic Record System usage, the private provider is required to have the employee receiving access to complete all Electronic Record System training noted on **CS-0944, Electronic Record System Access Request for Providers**.

NOTE: **CS-0944, Electronic Record System Access Request for Providers** includes all required Electronic Record System training associated with access levels and link to complete each training.

h) The private provider is responsible for maintaining **CS-0944, Electronic Record System Access Request for Providers** and required training records for all employees with the Electronic Record System access.

2. Change in Access to the DCS Electronic Record System Request:

a) When a current private provider employee (non-DCS employee) requires a change in the Electronic Record System access, the private provider supervisor/designee sends an updated **CS-0944, Electronic Record System Access Request for Providers** to **EI-DCS.ProviderRelations@tn.gov** identifying the change in access needed.

b) When completing **CS-0944, Electronic Record System Access Request for Providers**, the private provider is responsible for notifying ODGA of any modifications to current the Electronic Record System access, as applicable.

Example: Private provider employee is changing from a supervisor role to a case manager role; the private provider must update the access level to remove supervisory access and request only case manager access.

c) ODGA completes a SNOW Electronic Record System request, which routes to STS FCCR to update the user's access according to **CS-0944, Electronic Record System Access Request for Providers**.

d) When a change in access results in access to new modules in the Electronic Record System, the private provider employee completes Electronic Record System training for the newly granted modules.

NOTE: All employees can access Electronic Record System training online or through the Office of Training and Professional Development at **https://www.tn.gov/dcs/for-providers/tfacts-and-training/tfacts-help-documents.html**.

e) The private provider is responsible for notifying ODGA immediately if they discover an employee has access that should not be authorized or of any conflicts of interest with an employee's access levels.

f) All Electronic System requests will be maintained/archived in SNOW. STS will maintain/archive the accompanying **CS-0944, Electronic Record System Access Request for Providers** authorizing the change in SharePoint.

3. Termination of Access to the DCS Electronic Record System Request:

a) Private provider staff account access will be suspended automatically after 60 (sixty) days of inactivity, and the account will be terminated completely after 90 (ninety) days of inactivity.

b) On the same day of an employee's separation from the private provider, the private provider submits completed **CS-0944, Electronic Record System Access Request for Providers** to **EI-DCS.ProviderRelations@tn.gov** to terminate the employee's access to the Electronic Record System.

c) ODGA completes a SNOW Electronic Record System request, which routes to STS FCCR to terminate the private provider employee's access to the Electronic Record System within 24 (twenty-four) hours of receiving the form.

d) If the employee is terminated on the last day of the week, ODGA will contact STS FCCR directly, in addition to the e mail to STS, to ensure the FCCR is aware and can terminate access to the Electronic Record System on the same day before the weekend starts. This is non-negotiable.

e) All Electronic Record System requests for terminating a private provider employee's access will be maintained/archived in SNOW. STS will maintain/archive the accompanying **CS-0944, Electronic Record System Access Request for Providers** authorizing the termination in SharePoint.

4. Audit of Private Provider Employee Access to the DCS Electronic Record System:

a) The Electronic Record System has a module entirely devoted to creating, updating, and maintaining employee information, to include their Electronic Record System security. Security level(s) on this screen will match the employee's access as submitted on **CS-0944, Electronic Record System Access Request for Providers**.

b) Quarterly, ODGA sends an automated reminder to all private providers to send a list of active employees with Electronic Record System access.

c) ODGA reviews submitted lists with the internal records to ensure only current private provider employees have access to the Electronic Record System.

d) For employees not on the list and/or with unauthorized access, the private provider is notified and has one (1) business day to submit an updated **CS-0944, Electronic Record System Access Request for Providers** to ODGA.

Note: Failure to submit an updated **CS-0944, Electronic Record System Access Request for Providers** will result in immediate termination of employee access in the Electronic Record System.

e) ODGA completes a SNOW Electronic Record System request, which routes to STS FCCR to update the private provider user's access in the Electronic Record System within one (1) business day of receiving **CS-0944, Electronic Record System Access Request for Providers**.

f) STS FCCR notifies the ODGA of the former private provider employee's termination in the Electronic Record System within one (1) business day of completion.

g) ODGA ensures all former private provider employees' access is terminated.

h) At any time, a private provider user's usage in the Electronic Record System can be viewed for security purposes.

i) The Electronic Record System runs a script nightly that automatically suspends any user's access if user has not logged into the Electronic Record System for 60 (sixty) calendar days

Forms:

CS-4287 Electronic Record System Request for DCS Employees

CS-0944, Electronic Record System Access Request for Providers

Collateral Documents:

ServiceNow FAQs

New Report and Data Request Form

Data Issue, Correction, or Modification Form

STS FCCR Coverage Map