POLICY # 123	SUBJECT: User Access
EFFECTIVE DATE: September 7, 2021 REVISION DATE:	Page 1 of 4
Approved By: Josette Manning, Cabinet Secretary	

DELAWARE CHILDREN'S DEPARTMENT POLICY

I. PURPOSE

The purpose of this policy is to establish for employees, contractors, vendors and authorized users, consistent standards and processes for access to Department of Services for Children, Youth and Their Families (DSCYF) network, IT systems, applications and data.

II. POLICY

Protecting access to IT systems and applications is critical to maintaining the integrity of the department's technology and data and preventing unauthorized access. Access to technology, including networks, systems, applications, computers, and mobile devices, is restricted to only authorized users based on the principles of *need to know* and *least privilege.*

III. DEFINITIONS

A. *Need to know* principle: grant users only the rights and permissions they need to perform their job and no more.
B. *Least privilege* principle: grant users access only to the data they need to perform their job and no more.
C. *Electronic Employee Access Request Form*: http://dscyfform2/mis/forms/dscyf-user-access-form.pdf

IV. PROCEDURES

A. Requests for user accounts and access privileges must be formally documented and approved using the following procedure:
  a. The supervisor of the employee will initiate the electronic DSCYF Employee Access Request Form when a new employee is hired. No paper forms will be accepted.
  b. The supervisor will identify the access needed for the employee, including FOCUS access.
  c. If the new user is a temp, intern, contractor, or vendor, the designated DSCYF supervisor will ensure DTI Acceptable Use and DSCYF Confidentiality Policies (Policy 205) are reviewed, signed, and retained on file.
    i. If the contractor or vendor requires a DSCYF email address, the "needs DSCYF email" box must be checked.
    ii. The signed policies and the User Access Form will be emailed to the Helpdesk.

   iii. No access will be provided until all required forms and signatures are submitted.
   iv. Annual renewal is required.
- **d.** The supervisor will fill out the required information, sign, and submit according to the instructions on the form.
- **e.** The Helpdesk will process the request for network and IT systems access.
- **f.** If FOCUS access is required, the Helpdesk will forward to the appropriate division product owner.
   i. User access will be granted only to the specific resources the employee needs to complete their job duties.

B. Changes to user access for an existing employee must be formally documented and approved using the following procedure:
- **a.** When an employee's information changes (name, assigned supervisor, work location, phone number, job title, access updates), the supervisor must complete the electronic Employee Access Request Form.
   i. If the employee is changing supervision, the new supervisor is responsible for submitting the form prior to the effective date of the change.
- **b.** The supervisor will follow the steps outlined in section IV(A) above, ensuring that the FOCUS section of the form is updated if the employee is a FOCUS user. The employee should never have more FOCUS access than they need to perform their job duties.

C. If an employee's access must be immediately disabled due to suspension, being placed administrative leave, or temporarily ceasing to have a legitimate reason to access DSCYF technology, the supervisor must use the following procedure:
- **a.** Immediately notify the following by email: the Helpdesk, the appropriate division product owner, and Human Resources Labor Relations (DSCYF_Labor_Relations@delaware.gov). Access will be immediately disabled.
- **b.** When/if the employee returns to work, the employee's supervisor will immediately notify the following in writing: the Helpdesk, the appropriate division product owner, and Human Resources Labor Relations (DSCYF_Labor_Relations@delaware.gov). Access will be enabled.

D. If an employee separates from the department, the supervisor must use the following procedure:
- **a.** Submit the electronic DSCYF Employee Access Request Form no later than the date of separation to permanently disable access to network, IT systems, user applications and data, following the procedures outlined in IV(A) above.
- **b.** If the employee is a FOCUS user and has tasks on their worklist and/or cases on their caseload requiring transfer due to separation, the employee's access must be frozen before access is permanently disabled. A DSCYF FOCUS liaison must be notified no later than the date of separation to freeze the user's access.
   i. Worklist or caseload transfers must be completed within 5 business days of the employee's separation by the separating employee's supervisor/manager.

ii. The employee's supervisor/manager will immediately notify the division product owner once the worklist and/or caseload data is transferred.

iii. The employee's FOCUS user account will be permanently disabled by a DSCYF FOCUS liaison.

E. Information systems monitoring

a. In accordance federal, state and department policies, DSCYF audits user access and traffic patterns to identify inappropriate and/or unauthorized access to data and other privileged or sensitive information.

b. Suspicious activity identified during an audit is submitted to DSCYF leadership for review and analysis to determine if the activity was appropriate and related to a business need or if the activity was inappropriate and/or unauthorized.

c. Access determined to be inappropriate and/or unauthorized may lead to administrative inquiry and appropriate administrative, disciplinary, and/or legal action against the employee.

V. RESPONSIBILITY FOR THIS POLICY

The Division of Management Support Services is responsible for guidance relating to this policy.