PerformCARE®

Instructional Guide for CYBER Security Administrators

February 2024 – (02236)

Instructional Guide for CYBER Security Administrators

Table of Contents

I. Introduction

This guide's purpose is to define the functions of the Security Administrators' work and guide them in managing their users in CYBER. CYBER Security Administrators perform the role that manages and restricts access to an agency's users in the CYBER system.

When an agency becomes a Children's System of Care provider, each staff person must have their own Username to log in and use CYBER. The agency submits the contact information of one or two staff who will take on the role of Security Administrators by sending a written request to the PerformCare Service Desk. Additional Security Administration may be added upon written request. The Service Desk will reply with an email indicating the Security Administrators' set up.

The PerformCare Service Desk is the only entity with the ability to assign the security groups needed for Security Administrators; that role cannot be created at the agency level.

II. Responsibilities of CYBER Security Administrator

All CYBER users play a role in supporting PerformCare's security processes to safeguard Protected Health Information (PHI) in the New Jersey Children's System of Care. This is part of the Standards for Privacy of Individually Identifiable Health Information, as a requirement of the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') and federal confidentiality rules under 42 CFR Part 2.

The Security Administrators' primary responsibility is to manage their agency's user security in CYBER. This requires the administrators to know their staff, follow their own agency security protocols – personal information collection, background checks, etc., prior to providing a Username to a new user. Staff may be set up with their own caseloads and instructed how to properly access youth records to ensure HIPAA compliance. The Service Desk is always available for assistance.

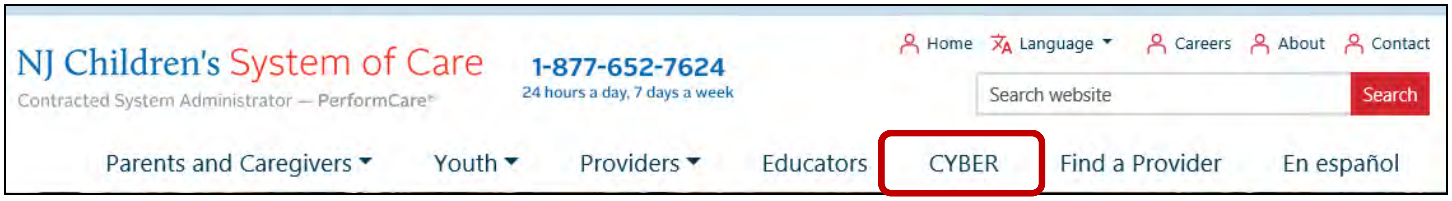
The responsibilities of the Security Administrator include the following:

- Creating new usernames
- Modifying existing usernames
- Deactivating usernames
- Reactivating usernames
- Assisting locked out users with password reset functionality
- Reviewing the roster of users in the organization that have access to CYBER and update their access on a routine basis.

To ensure HIPAA compliance, if the Security Administrator is no longer able to fulfill the responsibilities of the role, it is the agency's obligation to identify a new Security Administrator.

III. Accessing CYBER

CYBER can be accessed via the PerformCare website – www.performcarenj.org . The link is available under the CYBER menu at the top of the home page or the button at the bottom of the page. Users must log into CYBER with their Username and Password.



Each provider organization has at least two CYBER Security Administrators, and your agency's CYBER Security Administrators can set up a login and temporary password. Access will be based upon login type and security levels.

Before logging in, keep in mind…

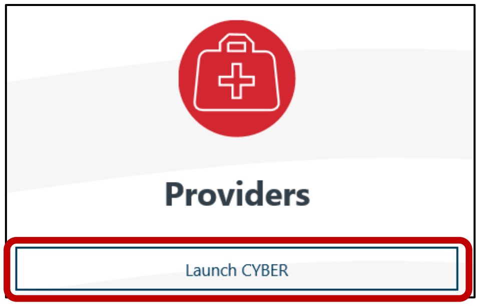
- Every time CYBER is launched, the **Username and Password is required, then click the LOGIN button to continue**.
- Users are required to **change their password every 90 days.**

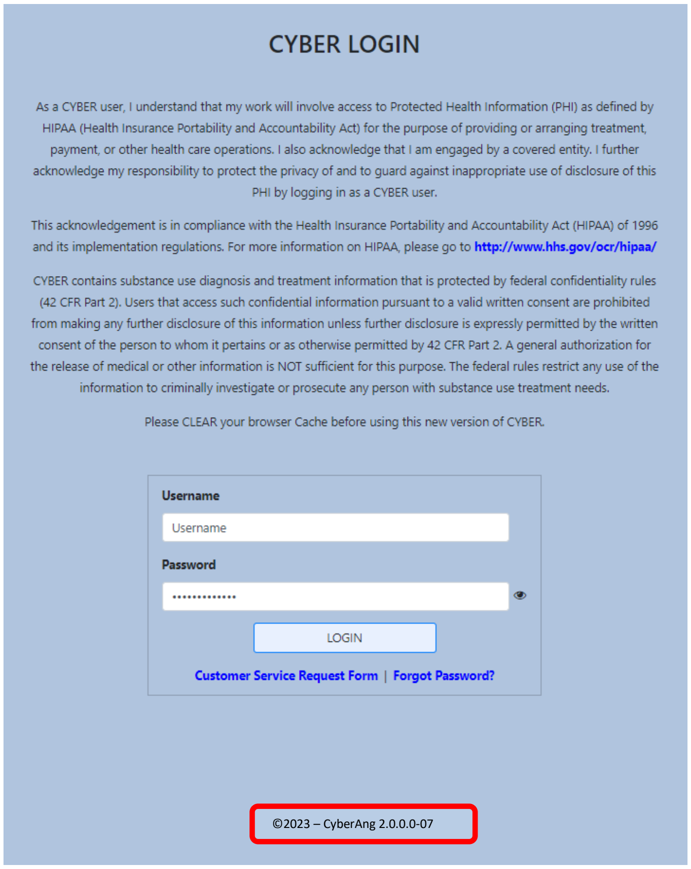
Above the login area is a statement that, CYBER users acknowledge their responsibility to protect the privacy of and to guard against the inappropriate use or disclosure the Protected Health Information (PHI) contained within the system.

This statement will appear during each log in.

Please also check the link: **CYBER Access Requirements** page on the PerformCare website for the most up-to-date technical requirements (such as browser compatibility and operating systems) needed to access CYBER.

At the bottom of the login page is the version of CYBER. The server number is the last 2 digits at the end (-XX). This is helpful to note when requesting assistance.





CYBER LOGIN

As a CYBER user, I understand that my work will involve access to Protected Health Information (PHI) as defined by HIPAA (Health Insurance Portability and Accountability Act) for the purpose of providing or arranging treatment, payment, or other health care operations. I also acknowledge that I am engaged by a covered entity. I further acknowledge my responsibility to protect the privacy of and to guard against inappropriate use of disclosure of this PHI by logging in as a CYBER user.

This acknowledgement is in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementation regulations. For more information on HIPAA, please go to **http://www.hhs.gov/ocr/hipaa/**

CYBER contains substance use diagnosis and treatment information that is protected by federal confidentiality rules (42 CFR Part 2). Users that access such confidential information pursuant to a valid written consent are prohibited from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any person with substance use treatment needs.

Please CLEAR your browser Cache before using this new version of CYBER.

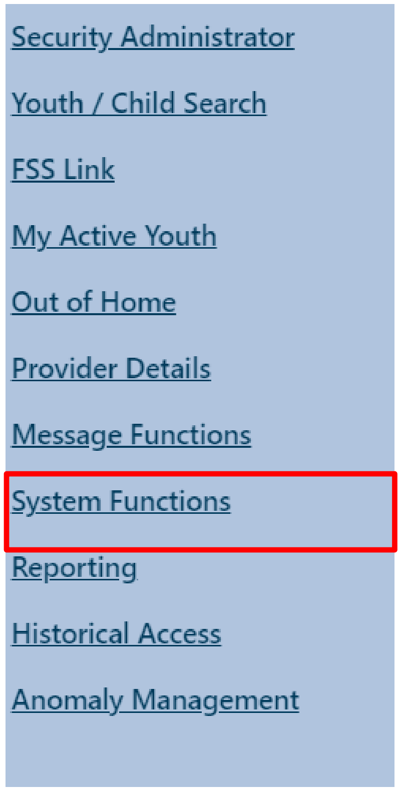
Username
Username
Password
••••••••••••••

©2023 – CyberAng 2.0.0.0-07

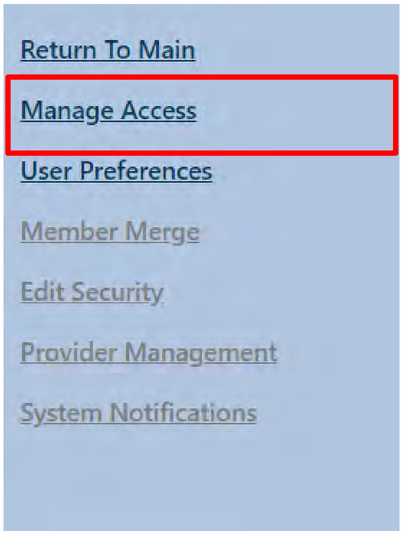
For technical support, please use the **Customer Service Request Form** link under the login.

IV. Accessing Security Administration

Security Administrators manage access by clicking on the **Systems Functions** link which is located on the left side of the user's Welcome Page.

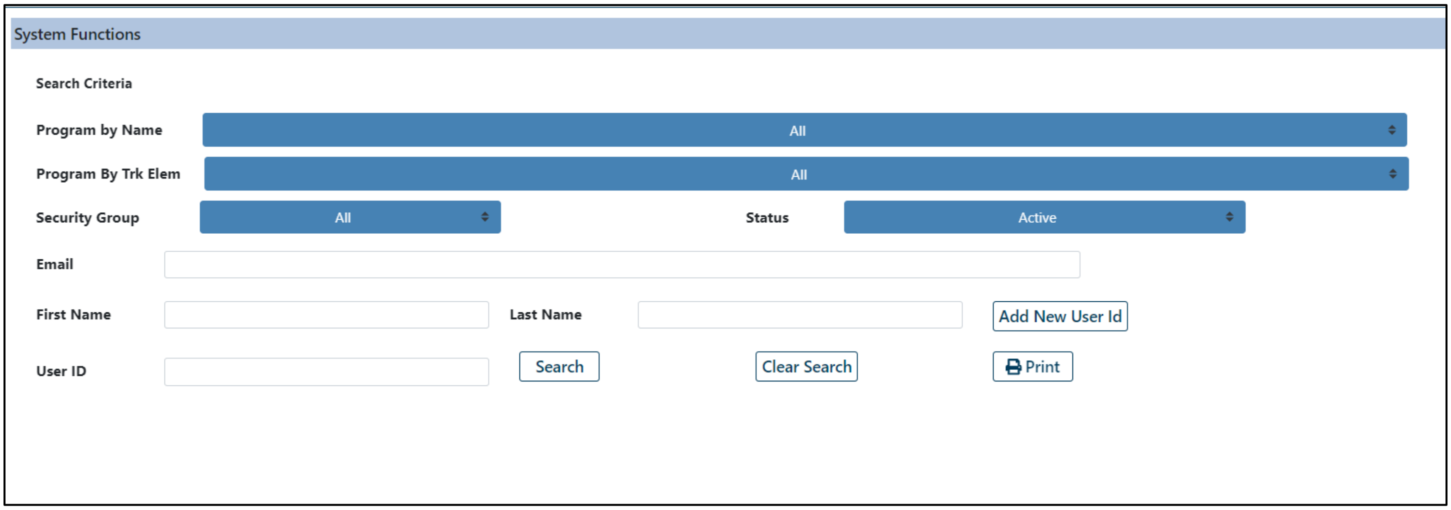


This brings users to the System Functions screen. The user then selects the **Manage Access** link from the left-hand corner of the window which will display the System Functions screen (Users not designated as Security Administrators, will be brought to their own Edit window, where they can change their own password.).



System Functions Screen

This is the main screen that allows Security Administrators to perform their responsibilities in CYBER. The search criteria fields are as follows (‘All’ is the default for dropdown fields. “Active “is the default for Status):



System Functions

Search Criteria

Program by Name: All

Program By Trk Elem: All

Security Group: All

Status: Active

Email

First Name

Last Name

User ID

- **Program By Name**: A list of the programs assigned to that agency
- **Program By Trk Elem**: A list of the Tracking Element names for the programs assigned to the agency
- **Security Group(s)**: A list of all the security groups that are available for the program(s)
- **Status**: Status identifies the status of the users at the agency (Active, Inactive, and All). All lists both active and inactive
- **Email**: The user should have a properly formed email address entered into their profile (partial entry for search is available)
- **First Name**: First name of the user (partial entry for search is available)
- **Last Name**: Last name of the user (partial entry for search is available)
- **User ID**: Username assigned to the user (partial entry for search is available)

Proper Formation of an Email Address

The proper formation of an email address includes an account name or username, the ‘@’ symbol and an email domain name with a top-level domain such as .com, .net, .org, etc. For example:

myname@domain.org

The buttons are defined as follows:

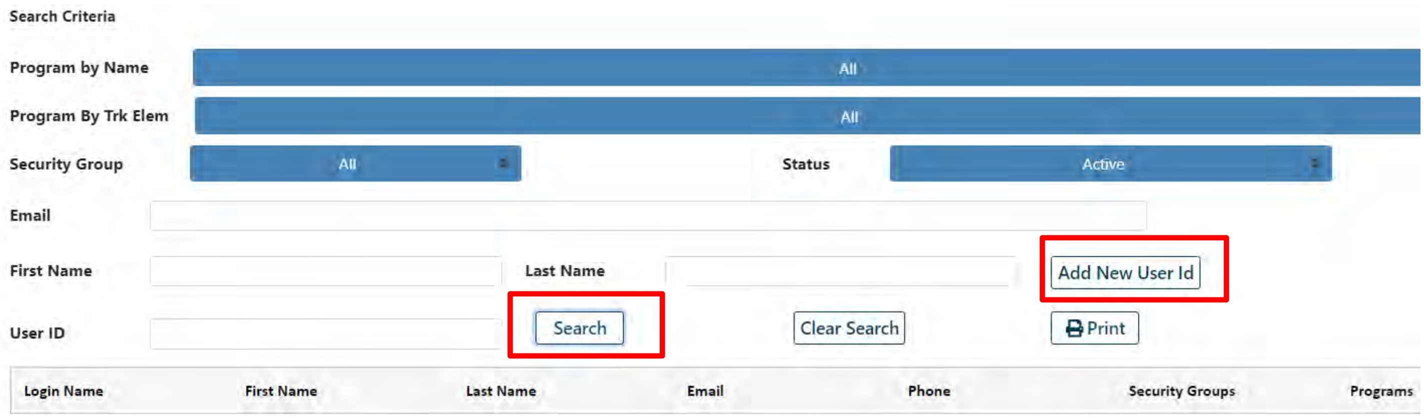
- **Add New User ID**: Allows Security Administrator to create a new username and add it to any of the programs open to the Security Administrator
- **Search**: Runs a search of the system based upon the Search Criteria entered
- **Clear Search**: Clears all Search Criteria fields and returns to the default settings
- **Print**: Allows Security Administrator to print the information displayed in the grid after a search

V. Creating a New Username

Before creating a new Username, the Security Administrator must:

- **Run a search for an existing Username** by leaving all text fields blank and the dropdown fields with default settings (All), and just click the Search button, keeping in mind that the system will return all usernames that are associated with the program(s) regardless of status (Active/Inactive).
- **If no user exists**, they can proceed with creating a new id

Once the Security Administrator has completed the Search and has clicked the 'Search' button, the grid below the search area will populate with the search results if available.



Search Criteria

Program by Name: All

Program By Trk Elem: All

Security Group: All

Status: Active

Email

First Name

Last Name

User ID

Login Name	First Name	Last Name	Email	Phone	Security Groups	Programs

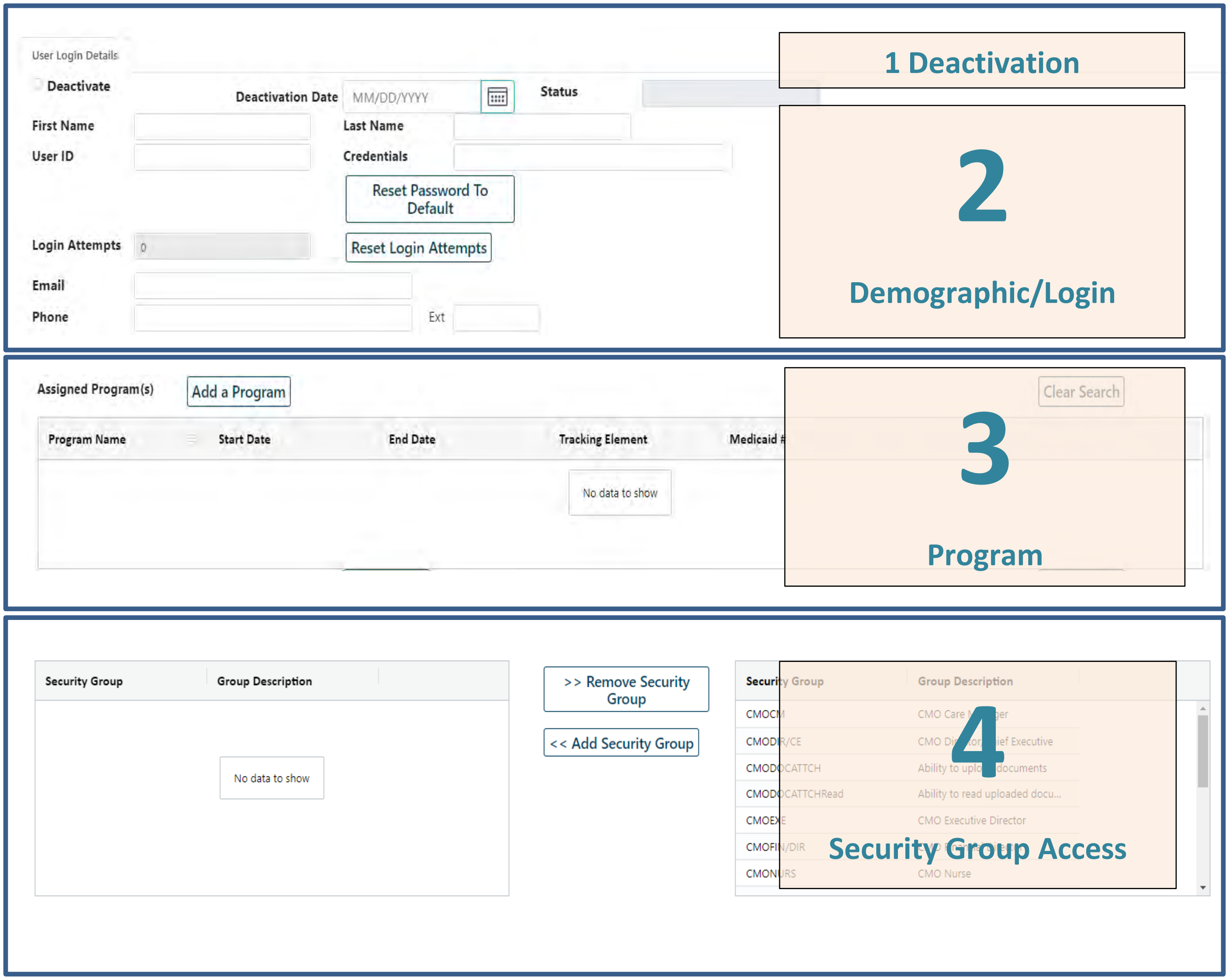
Search results appear in the grid

If no results are returned, the Security Administrator will click the **Add New User ID** button on the right hand side to open a blank User Login Details screen and begin a new Username. If results appear follow the instructions in **Modifying an Existing Username**.

Security Administrators can double-click the record in the grid and the User Login Details will open and display the user information.

The User Login Details screen is separated into four distinct areas:

1. Deactivation functionality.
2. Demographic/log in information.
3. Program information.
4. Security Group Access information.



User Login Details

○ Deactivate

Deactivation Date MM/DD/YYYY

Status

First Name

Last Name

User ID

Credentials

Login Attempts 0

Email

Phone

Ext

Assigned Program(s)

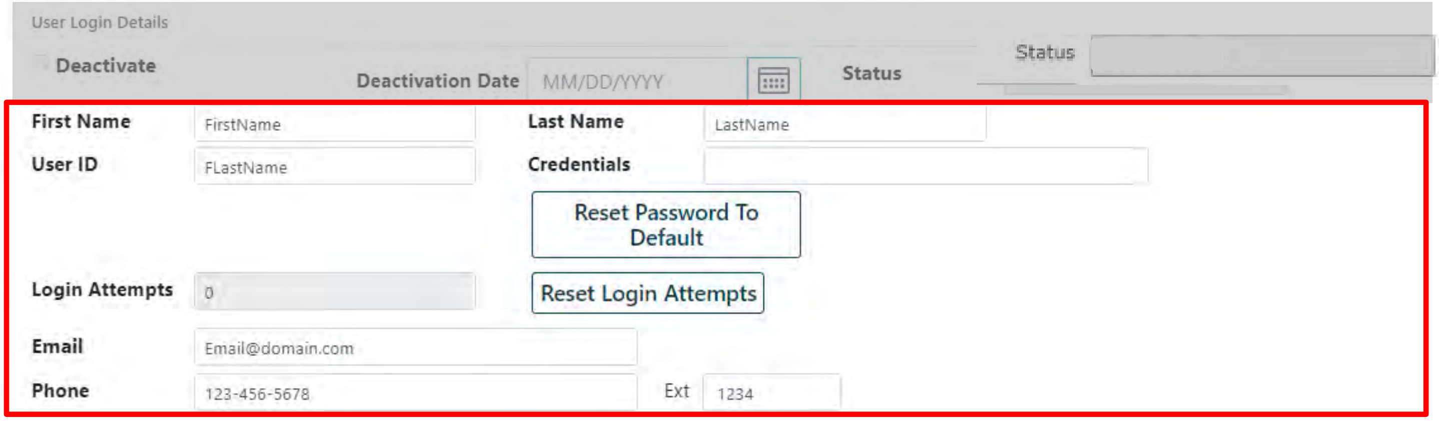
Program Name	Start Date	End Date	Tracking Element	Medicaid #
			No data to show	

Security Group	Group Description
No data to show	

Security Group	Group Description
CMOCM	CMO Care Manager
CMODIR/CE	CMO Director/Chief Executive
CMODOCATTCH	Ability to upload documents
CMODOCATTCHRead	Ability to read uploaded docu...
CMOEXE	CMO Executive Director
CMOFIN/DIR	CMO Financial Director
CMONURS	CMO Nurse

Demographic/Login information

The Demographic or Login information section identifies the user and the contact information for the user. The Security Administrator must complete all the fields to create a new Username. The fields and buttons are defined as follows:



User Login Details

Deactivate

Deactivation Date MM/DD/YYYY

Status

Status

First Name: FirstName

Last Name: LastName

User ID: FLastName

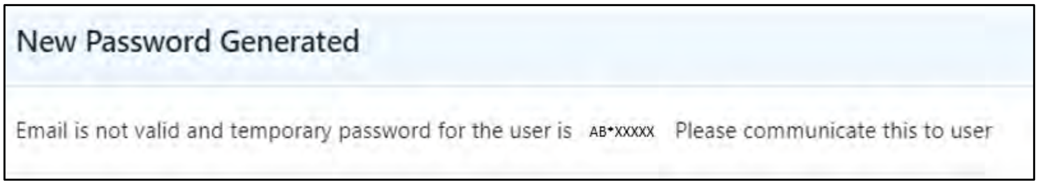
Credentials:

Login Attempts: 0

Email: Email@domain.com

Phone: 123-456-5678 Ext 1234

- **First, Last Name**: First and Last Name of the user (editable in case of name change).
- **User ID (Username)**: The unique username created to identify the user. Once created and saved, it cannot be edited. Suggested format is first initial, last name with a number (ex. bsmith2). Never share Usernames.
- **Credentials**: The clinical credentials of the user (LCSW, LSW, etc.); will be used in the future to automatically populate other areas of the system; information can be entered here if the agency choses to do so.
- **Password**: This field will be blank. Once set, the password will be masked for protection. Never share passwords.
- **Reset Password to Default**: Clicking this button will reset the user's password.
  - **If there is an email address for the user in the system** (see Email below), once Save or Save and Exit is clicked, the system will send the user a new temporary password.
  - **If the Email field is left blank** it is considered 'invalid', the user's password will be reset. The security administrator will receive a pop-up with a unique password reset for that user. Security Administrators will need to provide the password reset to the user; the user will not receive notification. The change will not take effect until Save or Save and Exit has been clicked.



New Password Generated

Email is not valid and temporary password for the user is AB•XXXXX Please communicate this to user

All users are required to have an active email and phone number entered into CYBER as contact information. This is essentially to access and receiving important communications from PerformCare.

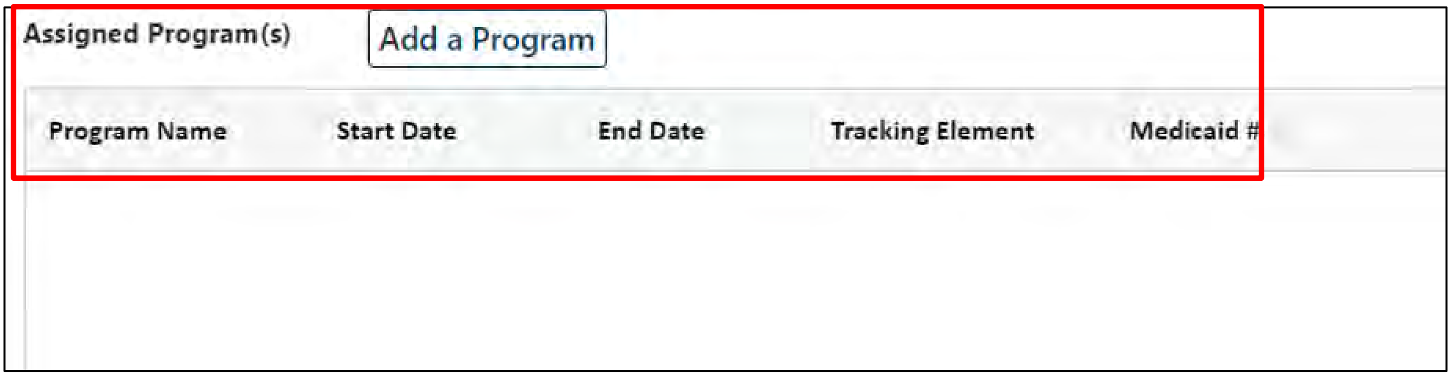
- **Login Attempts**: Lists the number of login attempts the user has had in one session before locking their account (can only be cleared, not edited). **The user has a maximum of 5 attempts before the username is locked** and the user may use their email address to reset their own password. Take care in entering user emails. If the user email address is entered incorrectly or the user does not have a valid email address in their user profile, they cannot reset their own password. They must contact their Security Administrator for assistance.
- **Reset Login Attempts**: Security Administrators may use this button to clear the user's attempts on their login. The user will need to refresh their browser before trying again.

- **Email**: The user's email address (editable by the user or administrator).
- **Phone**: The user's phone number (editable by the user or administrator).

Program Information

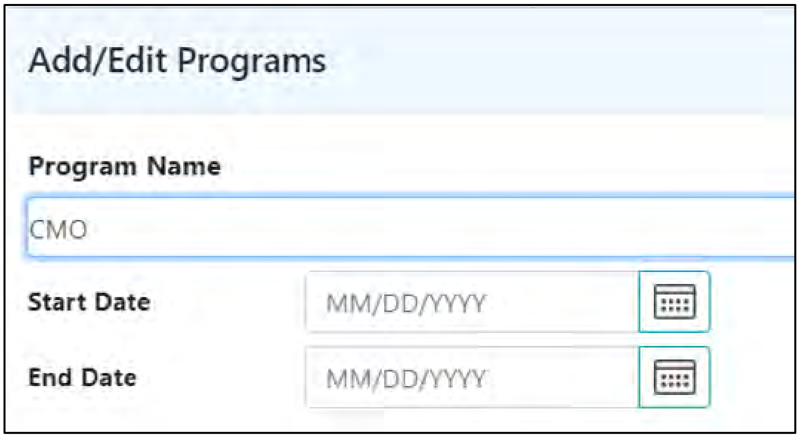
The Program Information identifies the programs that are open to the User. This feature allows youth IDs to be seen by users at an agency.

In the Assign Program(s) section, the Security Administrator should click the '**Add a Program'** button to bring up one or more programs that the Administrator has access to and can assign to other users.



The **Add/Edit Programs** window will open and allow the Security Administrator to add one program at a time to the user's Username; the Administrator must identify the user's Start Date. If the Security Administrator needs to end the user's access to one program without deactivating their access to CYBER, an End Date may be entered

The end date must be either today's date or a date in the future, it cannot be backdated.



Add/Edit Programs

Program Name: CMO

Start Date: MM/DD/YYYY

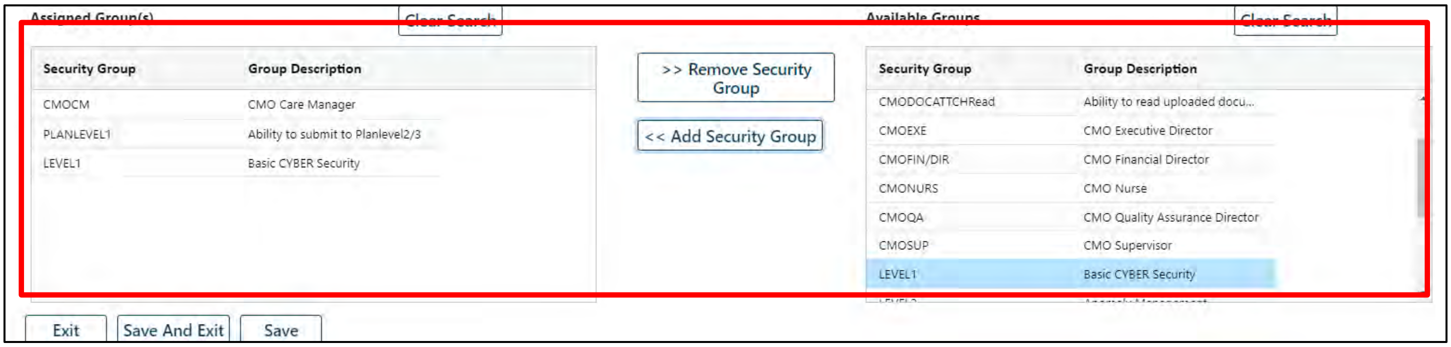
End Date: MM/DD/YYYY

The **Assign Program(s)** grid will be populated with any programs with which this user is currently associated. The grid will show the name of the program, the start date that the user gained access, an end date if the user is no longer associated with that program, the Tracking Element/Medicaid ID # of the program. (To deactivate a program from a user or a user from CYBER see **Deactivate a Username**.)

Once the Security Administrator clicks the 'Save and Exit' button in Add/Edit Programs, they will return to the Assign Program(s) grid and the newly added program will be listed.

The Administrator should always click Save and Exit before leaving the Username or changes will not be saved.

Security Group Information



Security Group	Group Description
CMOCM	CMO Care Manager
PLANLEVEL1	Ability to submit to Planlevel2/3
LEVEL1	Basic CYBER Security

Security Group	Group Description
CMODOCATTCHRead	Ability to read uploaded docu...
CMOEXE	CMO Executive Director
CMOFIN/DIR	CMO Financial Director
CMONURS	CMO Nurse
CMOQA	CMO Quality Assurance Director
CMOSUP	CMO Supervisor
LEVEL1	Basic CYBER Security

Below the Assign Program(s) grid, the Security Administrator will find the **Security Group information**.

Add Security Groups

For a new user, the Assign Group(s) area will be blank. To add security groups to the user's Username, the Security Administrator will go to the 'Available Group(s)' area on the right, click once on a group to highlight it, and click the 'Add Security Group button in the middle of the two grids. The new group will now appear on the left, in the Assign Group(s) grid.

The Security Groups that appear in the Available Group(s) grid that start with the agency type (CMO, CRI, etc.), have a **title** associated with them (Care Manager, Director, Supervisor, etc.). These should be assigned as they relate to the user's actual job title; this will dictate what the user can see in the Welcome Page Hierarchy (see Welcome Page Guide for High-Level Access)

The **Levels** in the security group list – **Level1, Level2, Level3** – pertain to the general security setup; these levels dictate what functions a user has access to. For example, Level1 allows general access to CYBER with no special functionality. Only Level3 users will have access to the Reporting button, while for specific agency types, Level2 and Level3 users will have access to the Anomaly Management screen.

Hierarchy or **Plan Levels** pertain to the user's ability to author a Treatment Plan or Assessment and submit it to another user in their agency for work or review. Not all agency types have access to all Plan Levels. For example, MST (Multi Systemic Therapy), FFT (Functional Family Therapy), PHP (Partial Hospital Providers) and CCIS (Children's Crisis Intervention Service) will only have PlanLevel3 available for use.

See Security Group Definitions specific to your agency.

- **PlanLevel1** – users can author plans, transfer them to other users within the organization or submit them to a user above them in the hierarchy (users with PlanLevel2 or 3) for submittal to the CSA. These users cannot submit directly to the CSA.

- **PlanLevel2** – users can author and accept transferred plans for review/edit, transfer them back to the author, and submit plans to another user above them in the hierarchy (PlanLevel3) and submit to the CSA.
- **PlanLevel3** – users can author plans, return plans to the originating user or submit plans to the CSA.

Remove Security Groups

The Security Administrator can select the group on the ‘Assign Group(s)’ grid and click on the ‘Remove Security Group’ button in the middle of the two grids. The group will be removed from the Assign Group(s) grid. Clicking the ‘Save and Exit’ or ‘Save’ button will save any changes made.

Security Group Names

The naming convention of specific service lines in the Available and Assign Group sections are listed in acronym form. See more acronyms in the Glossary at the end of this document.

Security Group Titles (alphabetical order)

- **ADM** – Security Administrator (this type security can only be added by the PerformCare Service Desk)
- **CM** – Care Manager
- **DIR/CE** – Director/Chief Executive
- **EXE** Executive Director
- **FIN** – Finance Officer
- **MGR** or **MGT** – Manager/Management
- **QA** – Quality Assurance
- **SUP** – Supervisor
- **WOR** Worker

SPECIAL NOTE For Supervisors, Managers, Directors, etc.: There is another type of hierarchy available on the Welcome Pages of Case Management Entities users. This hierarchy will allow users at the SUP, MGR, MGT, EXE levels to see the work of other users below their security on their Welcome Page; this is based upon the user’s organizational hierarchy.

Please refer to the previously released training located on the PerformCare website called Welcome Page Features for High-Level Access for more information on this functionality.

Security Groups with Specific Functions

There are special security codes for certain functionality, and for certain service lines. They are as follows:

- **Annex A Access –** available to OOH only
  - **AnnexA Admin Group** – allows user to access the Annex A area
  - **AnnexAEdit** – allows a user to create, edit, save, delete and submit Annex A Addendums for their program(s). Both
  - **Annex A Provider Read Only** – allows a user to read any of the Annex A Addendums that are in CYBER for their program(s).

Users must have AnnexA Admin Group with either AnnexAEdit or Annex A Provider Read Only to use the full functionality.

- **CMONURS** – used by CMO agencies that offer Behavioral Health Home (BHH) services; allows a Nurse within the CMO access to the Nursing Assessment and Quarterly Progress Update.
- **Doc Upload Access**
    - **DOCATTACH** – available to CMO, MRSS, IIC, IU, FSO and OOH; allows a user to upload and view certain documents within a youth's CYBER record.
    - **DOCATTACHRead** – available to CMO, MRSS, IIC, IU, FSO, and OOH; allows a user to view certain documents within a youth's CYBER record.

    Both DOCATTACH and DOCATTACHRead should be added together for full access.

- **IIH_ISS_Admin** – identifies ISS Security Administrators.
- **IIH_ISS_Plan** – used by IIH, gives a user access to the ISS Treatment Plan.
- **LinkSpec** – used by FSS providers, this allows a user with this code to edit the specifiers on their program's PIF.
- **ProviderDetailEdit** and **ProviderDetailEditSelf** – used by IIC and IIH/ISS providers to specify the counties, languages and specialties where they provide services.
- **SAMHSASurvey** – used by select CMOs that are participating in the SAMHSA Survey program.
- **Social Security Number (SSN) access** – used by CMO and MRSS
    - **SSN_3560_Read** – this security group allows users to <u>view</u> any SSN in the 3560 application.
    - **SSN_Update** – this security group allows users to update SSN on the Demographics tab and 3560 application.

Both SSN_3560_Read and SSN_Update should be added together. A maximum of 4 users may receive this security set.

VI. Modifying an Existing Username

When a Security Administrator needs to find a specific user to make a modification to their Username, entering criteria into the Search fields will narrow the search results. Users can also leave the fields at their default settings (All) and run a general search, keeping in mind that the system will return all users that are associated with all of the programs that the Administrator has access to within CYBER, regardless of status (Active/Inactive). Names will be default listed alphabetically by last name.

The Security Administrator must:

- **Search for the existing user**. Once the security administrator has clicked the 'Search' button, the grid below the search area will populate with the search results. Security Administrators can access the user's security screen by double-clicking on a record in the grid.

When the Username opens, Administrators are able to make any changes, and then click Save and Exit. If necessary, the user should be notified of any significant changes to their login.

As noted above, all existing username fields may be modified by the Security Administrator **<u>except for</u>** the Username.

VII. Deactivating a Username

When a user no longer works for an agency, it is required that the Security Administrator deactivate the user's access to CYBER as soon as possible so that the security and privacy of youth PHI that is housed in CYBER continues to be protected.

When to deactivate a Username:

- When a user leaves or is let go from an agency.
- If there is a user who is no longer with the organization but still has an active account in CYBER, this account must be deactivated <u>immediately</u>.
- A User who is on extended leave of absence should also have their account deactivated. A deactivated account can be reactivated when the user returns.
- If there are any HIPAA security concerns about the user, their Username should be deactivated.

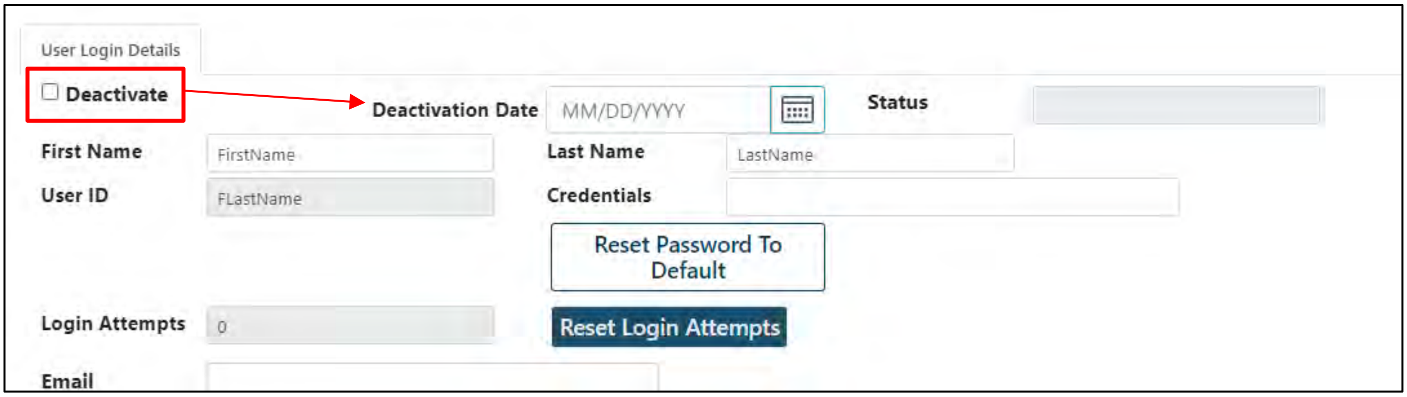
Note: When deactivating users, also end date the Provider Tab for any youth assigned to the deactivated user.

Deactivation Process

The Security Administrator will first need to search for the active Username. Once the correct user is located, the Security Administrator can then deactivate their access.

The Administrator should double-click the row with the identified name; it will open the record for that User. Putting a check in the 'Deactivate' box will prompt the system to display the current date in the Deactivation Date field; this date can be changed to a future date but cannot be backdated.

For the deactivation to take place in the system, the Security Administrator must click either the Save or the Save and Exit buttons at the bottom of the screen.



User Login Details

□ Deactivate

Deactivation Date: MM/DD/YYYY

Status:

First Name: FirstName

Last Name: LastName

User ID: FLastName

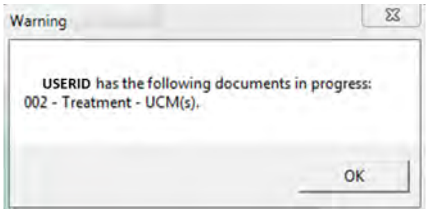
Credentials:

Login Attempts: 0

Email:

Exit
Save And Exit
Save

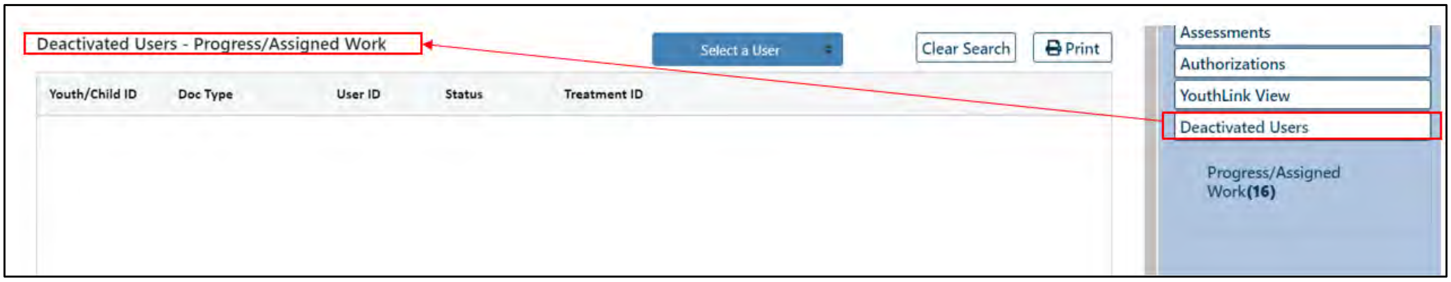
As soon as the Deactivate box is checked, the Security Administrator may receive a notification that the deactivated user has incomplete work (i.e. progress notes, plans or assessments, assigned to them that is in progress or in draft form).



USERID has the following documents in progress:
002 - Treatment - UCM(s).

Sample Deactivated user message.

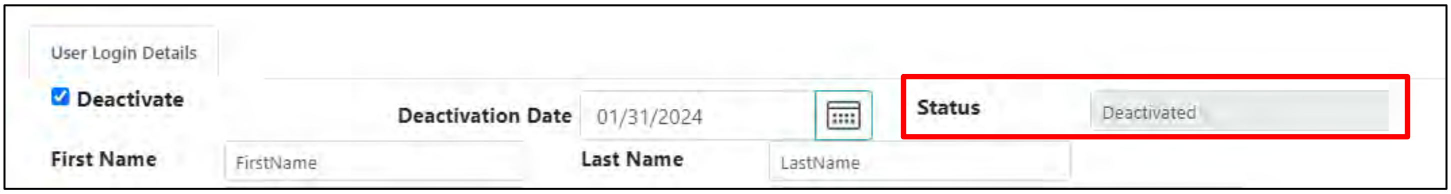
If this message is displayed, the Administrator may choose to alert the Supervisor of the deactivated user or the Manager (This step is optional). The Supervisor or Manager will now have access to the deactivated user's work via Deactivated Users accordion on their **Welcome Page**. For more information on these links, please refer to the training titled **Welcome Page Features for High-Level Access**.



Youth/Child ID	Doc Type	User ID	Status	Treatment ID

Sample of a CMO Welcome Page – Location of Deactivated Users in Progress information

VIII. Username Status



User Login Details

☑ Deactivate

Deactivation Date 01/31/2024

Status Deactivated

First Name FirstName

Last Name LastName

There is a read-only status field in the upper right corner of the User Login Details that defines the username's current status. Below is a table of the Status, the description of the activity that generated the status and action steps that are recommended.

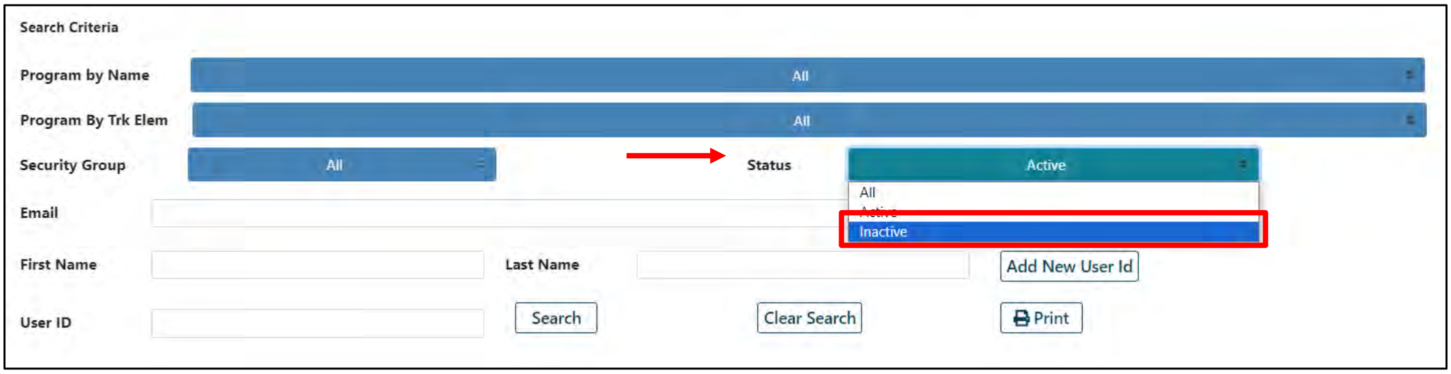
Status	Definition	Action
(field is blank)	Username is active	None needed
Password reset retries exceeded	User has attempted to reset the password by entering the email incorrectly 5 times	User has deactivated their account – Only the Security Administrator may reactivate
Login attempts exceeded	User has attempted to login by entering the password incorrectly 5 times	User is locked - user may reset account or Security Administrator may assist in password reset
Deactivated	Security Administrator has deactivated the account	User is deactivated – Only Security Administrator may reactivate if user returns to work. Review Welcome Page for unsubmitted work by the Deactivated User
Deactivated automatically	The username has reached the Deactivation date and the system automatically deactivated the username	User is deactivated – Only Security Administrator may reactivate. Review Welcome Page for unsubmitted work by the Deactivated User
90 Day User Lockout	User has not logged into CYBER for 90 consecutive days	Username automatically locked and user forced to reset their password to log back in.
180 Day User Deactivation	User has not logged into CYBER for 180 consecutive days	Username automatically deactivated; must contact the agency's Security Administrator(s) to reactivate their account

IX. Reactivating a Username

Security Administrators will need to know the two types of deactivations and how to reactivate the usernames.

- A user who has been deactivated by the Agency's Security Administrator
- A user who has deactivated themselves by using an incorrect email multiple times

In both situations, the Security Administrator should review the username to determine the next steps. In order to locate a user, the Security Administrator must first search for the user in CYBER. By entering information into the search criteria on the Manage Access window (Program Name, Tracking Element, First Name, Last Name, etc.), and then selecting 'Inactive' in the Status pull-down menu, will create a filtered search of only those usernames that are inactive that fit the search parameters. Click Search.



Search Criteria

Program by Name: All

Program By Trk Elem: All

Security Group: All

Status: Active

Email

First Name

Last Name

User ID

Once the all the inactive users' information appears in the grid, the Security Administrator can open the User Login Details screen by double-clicking on the selected record.

Agency-Deactivated Username

If the agency's Security Administrator has deactivated the username, they can follow these steps to reactivate:

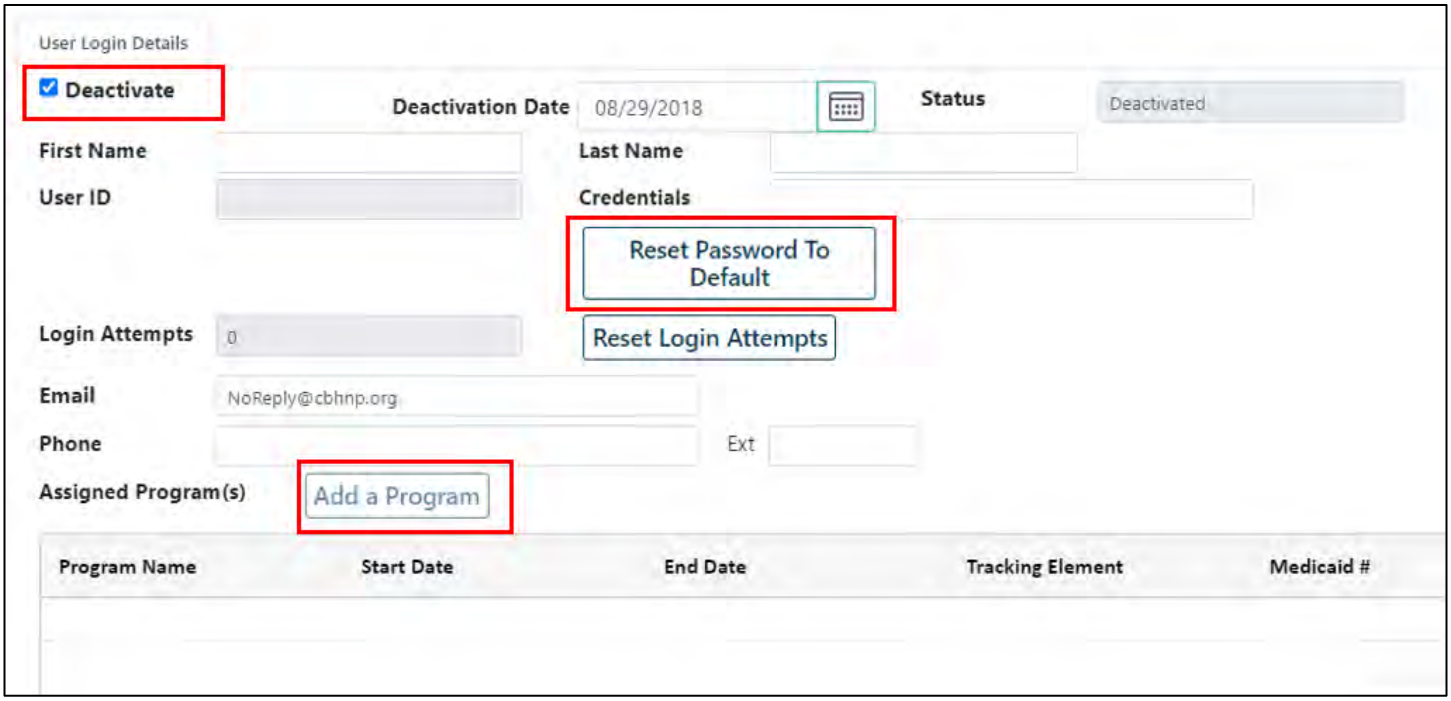
1. **Uncheck the Deactivate check box**: At the top of the User Login Details window, the Deactivate check-box will be selected; removing the check from the box will also remove the Deactivate Date and the Status (Deactivated)
2. **Click Add a Program:** (This button will be available once the Deactivate checkbox is removed) **Add** the appropriate program(s) and start date the user is returning to work
3. **Check the Security Groups**: (This area will be available when the Deactivate check box is removed) Make sure the user is returning at the same security, Plan Level, Level, etc.
4. **Check for or enter the Email address**: This is required and will allow the user to reset their own password
5. **Reset the user's password by clicking 'Reset Password to Default'**: This will display the message 'When you save these changes a temporary password will be sent to the email address below.'
6. **Check for any special security that may be missing:** When a user with SSN access becomes deactivated, the SSN security groups are removed from their username (see Security Groups with Specific Functions). The Security Administrator must add this security to the username to fully restore the functionality.
7. **Click Save and Exit**: This will save the changes and reactivate the user's Username

User-Deactivated Username

The user can become deactivated by entering their associated email incorrectly 5 times. This is described in the Instructional Guide for CYBER Password Reset Functionality.

The Security Administrator should use these steps to reactivate a user-deactivated username:

1. **Uncheck the Deactivate check box**: At the top of the User Login Details window, the Deactivate check-box will be selected; removing the check from the box will also remove the Deactivate Date and the Status (Deactivated)
2. **Click Reset Login Attempts**: This will clear the attempts the user made so they can login again
3. **Check for complete and accurate Email**: Enter the user's email if blank.
4. **Reset the user's password; click 'Reset Password to Default':** This will display the message 'When you save these changes a temporary password will be sent to the email address below.'
5. **Check for any special security that may be missing:** When a user with SSN access becomes deactivated, the SSN security groups are removed from their username (see Security Groups with Specific Functions). The Security Administrator must add this security to the username to fully restore the functionality.
6. **Click Save or Save and Exit**: This will save the changes and reactivate the user's Username.



User Login Details

☑ Deactivate

Deactivation Date: 08/29/2018

Status: Deactivated

First Name:

Last Name:

User ID:

Credentials:

Login Attempts: 0

Email: NoReply@cbhnp.org

Phone:

Ext:

Assigned Program(s):

Program Name	Start Date	End Date	Tracking Element	Medicaid #

X. Password Reset Functionality

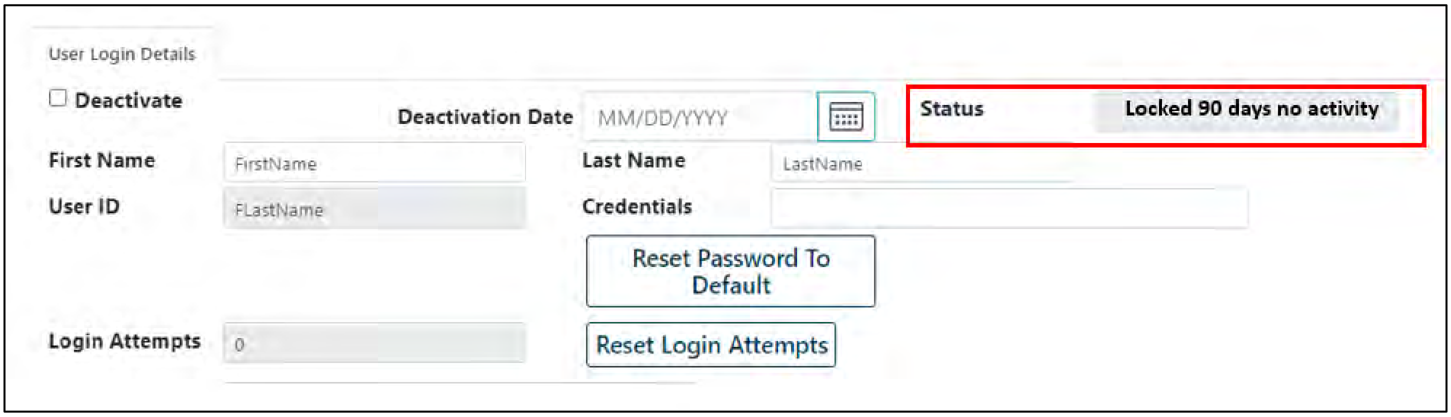
Many websites allow users to reset their passwords when they've either forgotten them, entered them incorrectly a number of times or when too many incorrect attempts at entering a password has locked their account. CYBER also has functionality that allows a user who has difficulty logging in, the option of resetting their password without having to contact the Security Administrator or the Service Desk.

It is required that when creating new users, the Security Administrators enter a user's current email address correctly into the email field so that the user may reset their own password at any time (see training **Password Reset for All Providers**).

90 and 180 Day Rules for User Lockout/Deactivation

A user may lock or deactivate their own username if they do not log into CYBER regularly.

If a user does not log into CYBER for 90 consecutive days, the username will be automatically **locked** and the user will be forced to reset their password to log back in. The system will display a message, 'Your account has been locked because you have not logged in 90 days. Please click 'OK' to reset your password', on the CYBER Login page if the status is 'Locked 90 days no activity'. Additionally, the system will display the status captured 'Locked 90 days no activity' on the User Login Details tab beside the Deactivation Date field.



User Login Details

☐ Deactivate

		Deactivation Date	MM/DD/YYYY
Status	Locked 90 days no activity		
First Name	FirstName	Last Name	LastName
User ID	FLastName	Credentials	
Login Attempts	0		

If a user does not log into CYBER for 180 consecutive days, the username will be automatically **deactivated**. When the user attempts to log in after 180 days, they will receive the message, 'Your username is no longer active. Please contact your security administrator'. The user should contact the agency's Security Administrator(s) to reactivate their account.

In this circumstance, the Security Administrator will note that the username has the deactivate checkbox and the date the user was deactivated, but the Added Program(s) will not have an End Date. The username may be reactivated by simply **unchecking the Deactivate** check box and **clicking Save or Save and Close**. The user should refresh their browser before attempting to log in again.

Reset the Password

When users have attempted to log in 5 times unsuccessfully (with the wrong password), Security Administrators will see the status 'Password reset retries exceeded' on the User Login Details tab. In this circumstance, the user has the ability to reset their own password using their associated email as long as the email is entered and valid. If either their email is missing or entered incorrectly, the Security Administrator will have to assist.

By entering information into the search criteria on the Manage Access window (Program Name, Tracking Element, First Name, Last Name, etc.), and then selecting 'Inactive' in the Status pull-down menu, will create a filtered search of only those usernames that are inactive that fit the search parameters. Click Search.

To reset the user's password, the Security Administrator should click System Functions/Manage Access buttons and search for the Username by entering information into the search criteria on the Manage Access window (Program Name, Tracking Element, user's First Name or Last Name, etc.) will create a filtered search of the data that fits the search parameters. Click Search.

1. **Status should be blank**: In the upper right corner the status should be blank indicating the username is active
2. **Click Reset Login Attempts**: Before clearing this field should show a number indicating attempts the user made to log in. Clicking this button will clear the attempts the user made so they can login again.
3. **Check for complete and accurate Email**: Enter the user's email if blank.
4. **To reset the user's password, click 'Reset Password to Default':** This will display the message 'When you save these changes a temporary password will be sent to the email address below.' (Message 1)

(If there is no email in the Email field, the message will display 'The email address below is not valid…' (Message 2). Check the Email field and reset the password again.

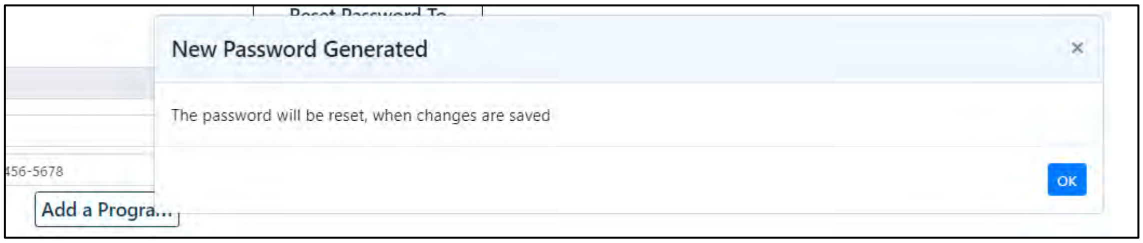
5. **Click Save or Save and Exit**: This will save the changes and reactivate the user's Username

After clicking **Reset Password to Default**

MESSAGE 1

Example of message when the user has an email.

Password sent to email is randomly generated.



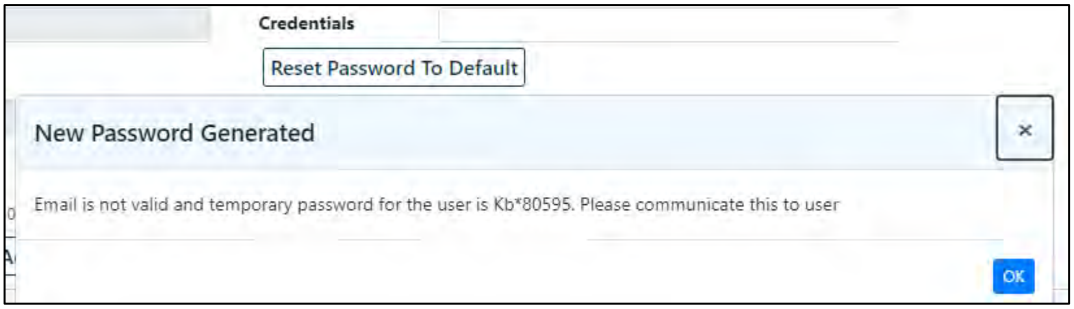
New Password Generated

The password will be reset, when changes are saved

MESSAGE 2

Example of message when the user has no email.

Password is not emailed, and **a unique password** will be created



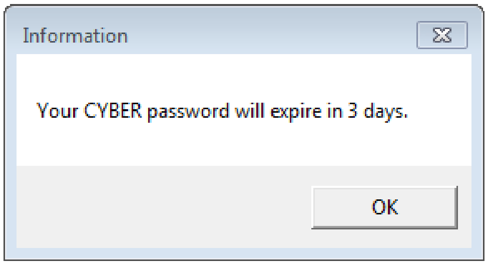
New Password Generated

Email is not valid and temporary password for the user is Kb*80595. Please communicate this to user

All users are <u>required</u> to have an active email and phone number entered into CYBER as contact information.

User should be instructed **to check their email for a temporary password, close all internet browser windows**, return to the PerformCare website, www.performcarenj.org and click *Launch CYBER* to refresh their browser.

Reminder Notification



Information

Your CYBER password will expire in 3 days.

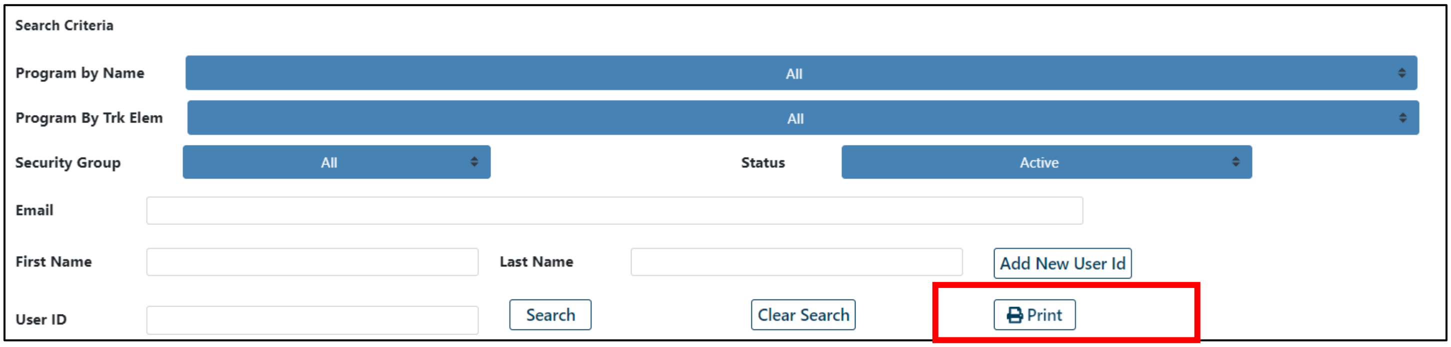
*CYBER will keep track of the last password change and will display a **reminder notification** when the password needs to be changed, 5 days prior to the 90 day limit. New passwords must be at least 8 characters long, with at least 3 out of the 4 following character types: upper case letters, lower case letters, numbers and/or special characters*. The system will remember and not permit reuse of users' last four passwords.

The reminder notification will occur when the user logs into CYBER.

While logged into CYBER, users can change their own passwords at any time by clicking on the 'Systems Functions' button on their Welcome Page and then the 'Manage Access' button. Direct users to the guide, Password Reset for All Providers.

XI. Exporting/ Printing

The Security Administrator can click on the 'Print' button to create a report of any list of users that were searched on and populated the grid. The report will appear in the View Report window, and will be exportable to a PDF file, Excel, Rich Text Format, and a TIFF File (see Glossary - Formats for Exporting or Printing).



Search Criteria

Program by Name: All

Program By Trk Elem: All

Security Group: All

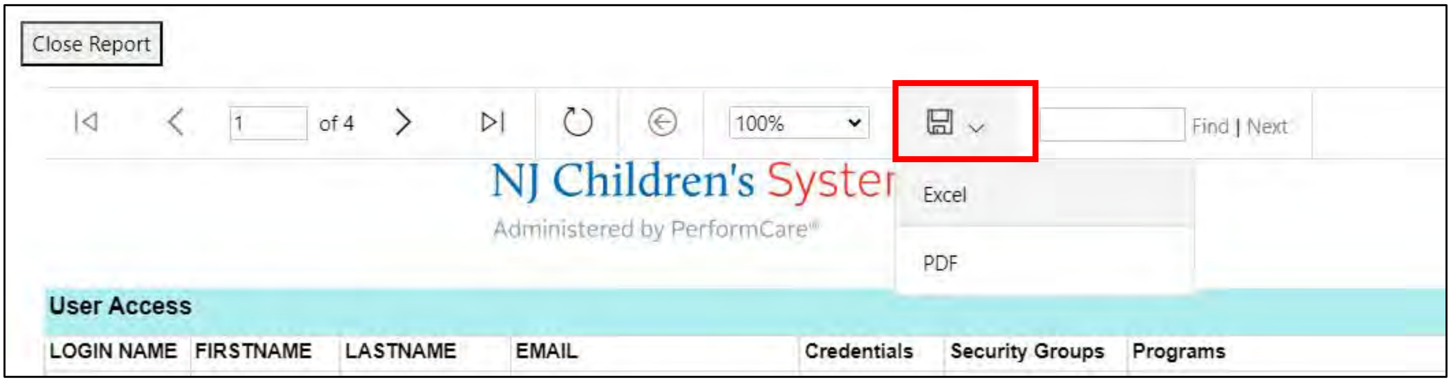
Status: Active

Email

First Name

Last Name

User ID



User Access

LOGIN NAME	FIRSTNAME	LASTNAME	EMAIL	Credentials	Security Groups	Programs

Administrators may click the **floppy disc icon** and pull-down selections for exporting. The document will download to the user's computer based on browser type. Once the file has been exported, users can print.

To return to the grid, the Security Administrator will click on the '**Close Report**" tab that is above the report window.

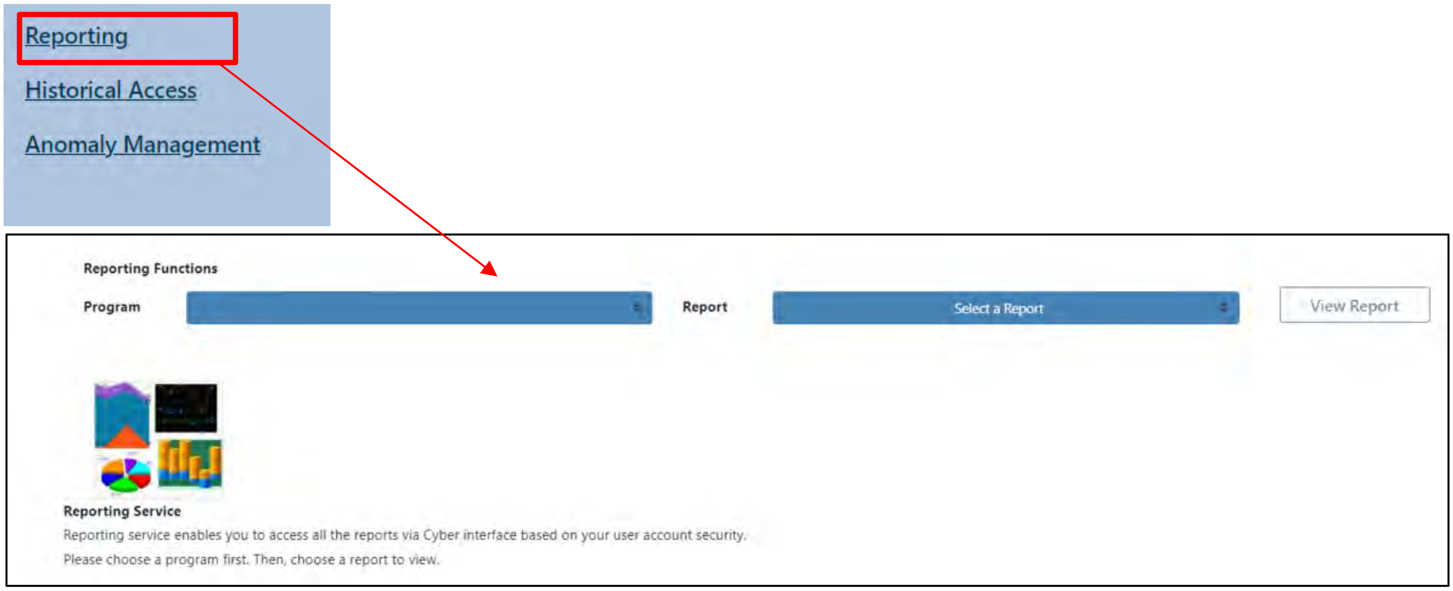
XII. Security Administrator Reports

Security Administrators must have Level3 security in their Username to have access to the Reporting button. There is a variety of reports available to Level3 users that generally assist in managing CYBER data.

To Search for reports, after logging into CYBER, click the Reporting link in the left-hand column. This will bring users to the Reporting Functions screen. Once a program is selected from the dropdown menu and a report is selected, the user can click View Report and view, export or print available reports.

To assist in managing Usernames, report **NJ1371_ManageAccess** is available to each Security Administrator with Level3 access. To view the report, click **Reporting** on the main menu of CYBER, and then select the associated program from the Program drop down and then choose **NJ1371_ManageAccess** from the Report menu.

As a part of PerformCare's security processes for safeguarding Protected Health Information (PHI) in the New Jersey Children's System of Care, it is **required** that you review the roster of users in your organization that have access to CYBER and update their access on a routine basis.



Reporting service enables you to access all the reports via Cyber interface based on your user account security.

Please choose a program first. Then, choose a report to view.

XIII. Troubleshooting

ISSUE	RESOLUTION
The password was reset but the user says they never got the email.	Confirm the user's email address and also check for a space anywhere in the user's email, especially at the end of the email. If there are any spaces remove them, click **Reset Password to Default** and click Save and Exit.
The password was reset but the user is still locked out.	The user must close all internet browser windows, then using Internet Explorer, navigate to the website, www.performcarenj.org and click the Launch CYBER and try to log in using the correct Login Name and password.
The Security Administrator is deactivated.	Follow instructional guide to reset the password, or contact your back up Security Administrator to unlock you. If you have no back up, contact PerformCare Service Desk at 1-877-652-7624.
User cannot see the correct person to submit a plan to.	Check PlanLevels – A user with a specific PlanLevel cannot submit to another user with the same PlanLevel.
User says s/he cannot create an assessment or plan.	At minimum, make sure the user has a Program with a start date, Security Group title, a Level and a PlanLevel.
User says s/he cannot see any youth in CYBER after logging in.	Check to make sure the user has a Security Group title and the correct Program is assigned to the user with a start date only.
Security Administrator created a Username with the wrong spelling of the person's name.	Security Administrator should deactivate the incorrectly spelled Username and create a new one.

XIV. Glossary

- Active – referring to a username being functional in CYBER
- Activate – to create a Username in CYBER and give access to a specific program and related data
- Anomaly Management – button on Welcome page that lists anomalies in youth records
- Auto-populate – function that enters predetermined data in a field when another action occurs elsewhere
- Back dated – when a request is made to start an action earlier than the present date (ex. tracking elements, authorizations, admissions, etc.)
- Button – a rounded box in CYBER that requires a single-click action
- Deactivate – (not currently active) the username is not functional in CYBER; deactivated by either the agency or by incorrect attempts to reset the password
- Double-click – Two clicks in quick succession; action usually performed on a row in a grid
- Drop down menu – a box that when single-clicked displays a list of items to select from
- Entity – an agency or provider or a named group (Service Desk)
- Grid – sections of CYBER data arranged into columns and rows
- HIPAA – Health Insurance Portability and Accountability Act – 1996 federal law that restricts access to individuals' private medical information
- Invalid – the password is missing, not formed properly or has extra spaces at the beginning or end
- Link – (aka hyperlink) a word or series of words that appear underlined; when single-clicked, brings the user to another location in CYBER

- Locked – a temporary state where the CYBER username is valid, but the password has been entered incorrectly multiple times requiring the password to be reset
- PHI – Protected Health Information – information that must be kept private by any health care provider.
- Profile – the details that make up a Username or login (ex. name, credentials, phone number, etc.).
- PerformCare Service Desk – technical support staff
- Program – a general term used to describe a specific agency, Medicaid or non-Medicaid group
- Reactivate – to modify a deactivated Username to make it active again
- Security group – a specifically named piece of code that allows certain kinds of functionality or access in CYBER
- Security Administrator – CYBER user with specific security that allows for creation of other agency usernames
- Welcome Page – The first page that appears after CYBER login (says Welcome to CYBER)
- Valid – the CYBER username exists or a password is formed correctly
- Window – a framed box-like shape in CYBER that pops open in front of the main view

Formats for Exporting or Printing

- PDF – Portable Document Format – an electronic **image of a document** with text and/or graphics that looks like a printed document.
- Excel – **spreadsheet** format with rows and columns, useful for reporting.
- Text Format – a file specifically formatted for **text documents that can be read by most word processors.**
- TIFF – Tagged Image File Format – file format that is adaptable for **handling images and data** like scans, faxes, optical character recognition, etc.

Agency Acronyms

- AHH - Adolescent Housing Hub
- CIS - Children's Crisis Intervention Service
- MRSS - Mobile Response and Stabilization Services
- CSA - Contracted System Administrator
- FFT - Functional Family Therapy
- FSO - Family Support Organization
- FSS - Family Support Services
- IIC - Intensive in Community
- IIH - Intensive In-Home
- ISS - Individual Support Services (a subset of IIH)
- IU – Intermediate Inpatient Unit
- MRSS - Mobile Response and Stabilization Services
- MST - Multi Systemic Therapy
- OAS - Office of Adolescent Services
- PHP - Partial Hospital Provider
- OOH- Out of Home
- SUT - Substance Use Treatment
- CMO - Care Management Organization

XV. References

- Password Reset for All Providers - http://www.performcarenj.org/pdf/provider/training/security/instructional-guide-password-reset-all-providers.pdf
    - Guide for all CYBER users to reset their own CYBER password

- Quick reference guide for CYBER Security Administrators – https://www.performcarenj.org/pdf/provider/training/security/role-based-security-system-admin-qrg.pdf
    - Basic guide to the main functions for Security Administrators

PerformCare Customer Service

www.performcarenj.org/ServiceDesk

1-877-652-7624