CDD Vault Policy And Procedures

Owner: Security Officer
Last updated: 1/5/2012

Policy Statement

Responsibility Assignment

While CDD support provides guidance and help, Vault administrators are fully responsible for the configuration and membership of their Vault. It is their responsibility to enforce this policy and monitor the Vault configuration, membership, and activities. In particular, user roles/privileges and user membership into projects need to be maintained regularly by the Vault administrators.

Support Requests

All support requests regarding configuration and membership management must be performed via emails to support@collaborativedrug.com or by submitting support requests on the CDD Support portal at https://support.collaborativedrug.com.

New Vault Setup

The Vault administrator is responsible to configure its Vault and create the initial projects.

Changes to Vault options that cannot yet be configured using the Vault Setting interface must be requested in writting to CDD support.

Identity Proofing

Before adding a new Vault member, the Vault administrator is responsible to first perform, or verify that the company's RA performed, identity proofing for the individual.

Least-Privilege Requirement

When assigning a Vault member role, the Vault administrator must choose the most restrictive role needed by the new user for the performance of specified tasks.

Vault Membership Management

Vault membership additions, removals, and modifications are performed by CDD support based on a written request by the Vault administrator.
The Vault administrator is responsible to monitor Vault membership notification emails sent by the CDD Database and verify the list of Vault members and roles (on the Members page of the Vault) after each change.

Regular Vault Membership Audit

The Vault administrator must regularly review the Vault members list in the "Manage Vault" section of the CDD Vault and make sure that the list is current and roles are correct. If something is incorrect, the Vault administrator must notify CDD support immediately to perform the necessary modifications.

Project Membership Management and Review

The Vault administrator must manage the initial project membership and continuously review the current project memberships.

Vault Activity Monitoring

The Vault administrator must monitor the vault activity log (see recent activities on the Dashboard) for strange activity and behavior; and report any issue to CDD support immediately.

Vault Members Policing

The Vault administrator must make sure that Vault members do not share their credentials and are aware of the security implications regarding access to the CDD Database.

Policy Applicability

All CDD Vault users with Vault Administrator role.

Related Policies and Documents

- Security Practices Overview (https://www.collaborativedrug.com/pages/security_practices)
- Security section of the CDD Support Portal (https://support.collaborativedrug.com)
- CDD Security Practices Whitepaper (distributed on a as-needed basis)

Procedures

New Vault Setup Procedure

CDD's standard process for new accounts includes a Vault administrator training and guidance session in which CDD teaches the vault administrator how users receive their accounts and what they will be able to do in the Vault.

New Vault setup includes the following steps:

1. The Vault administrator configures the Vault settings. Additional security settings can also be configured by CDD support upon written request.
2. The Vault administrator provides a written list of members, whose identity has been proofed, that includes first name, last name, email address, and assigned role.
3. CDD support adds these members to the Vault. Automated notification emails are sent to the new member and to the Vault administrator for each new member added.
4. The Vault administrator reviews the emails and the member list directly in the Vault to ensure membership and roles are correct.
5. The Vault administrator sets up projects in CDD with guidance from CDD support.
6. The Vault administrator assigns each member to their project(s) with the respective project permissions.
7. The Vault administrator can request CDD to set up the project membership on his/her behalf.
    a. The Vault administrator provides a written list of project membership assignments to CDD support.
    b. Upon completion of the request by CDD support, the Vault administrator verifies the correctness of the assignments

Please note: In collaboration projects where some Vault members do not have permission to see all data it is extremely important to assign all members correctly as the project assignment determines what a user is able to see or work on.

Ongoing Vault Membership Management

Each Vault membership addition, removal, or modification requires the following steps:

1. The Vault administrator sends a written request to CDD support with the necessary member credentials (first name, last name, email address, and role).
2. CDD support performs the membership modification. An automated notification email is sent to the Vault administrator.
3. The Vault administrator reviews the emails and the member list directly in the Vault to ensure membership and roles are correct.

User Credentials Recovery Procedure

CDD Vault users that have forgotten their password can reset it by using the password reset page accessible from the CDD vault login page (at https://app.collaborativedrug.com).

CDD Vault users sometimes do not remember their login ID. The ID typically is the user's email address but people have several and may still not remember. In this case, they can do the following:

1. Contact their Vault administrators that can check the Vault membership list and tell them which email is associated with their account.
2. Contact CDD Support. In this case, CDD support will have to proof the identity of the user via one of the following mechanisms:
    a. CDD can see the legitimate User ID (and therefore also email address) of the user in question. CDD will reset the password upon which a temporary password will be emailed to the email address associated with the account.
    b. If the user is a Vault administrator and claims to have a new email address, CDD support will contact the business owner to request identity verification using the contact information associated with the business contract.
    c. If the user is not a Vault administrator and claims to have a new email address, CDD support will contact the Vault administrators to request identity proofing. Once the user has been identified and the Vault administrator has confirmed the change request, CDD support will change the user email address and reset the associated password.

Second-Factor Authentication Phone Registration Procedure

Once the second layer of user authentication is activated, every single Vault user is required to register a mobile device or telephone the first time they access CDD.

Users must complete the following steps in order to authenticate their mobile device or telephone:

1. The user must log in using their secure CDD username and password.
2. User must register their phone by adding the number, specifying the type (mobile devices preferred) and selecting the verification method (text or call). The verification code is 4 digits long. If the user chooses to receive a call, the verification number is repeated 3 times.
3. Once the number is verified, the user can click continue.
4. The user is then presented with an option to either install Duo Mobile if they have a iPhone, Android, Palm, Blackberry, Symbian, J2ME, or Windows Mobile phone, or they can choose to skip this step. To install the program on the user's mobile device, simply click the button to text the installation link or show the QR code. If the user chooses to not install Duo Mobile, simply click the link to "skip this step."

Once the mobile device or telephone is registered and subsequently, every time the user attempts to log in CDD by supplying a valid username and password, the database will prompt the user to confirm they have access to the registered mobile device or telephone.

The user can complete this verification using one of the following methods:

- Duo Push (only available for Duo Mobile): notification is received and the user has the option to Approve or Deny the request. Once approved the user is logged in.
- Phone Call: Duo system will call the user's number and ask them to press any key to authenticate.
- SMS passcodes: Duo will send a batch of passcodes and the user must supply the correct one as indicated underneath the passcodes box on the CDD webpage.

Alternate Phone Registration Procedure

In order to register more than one telephone number to perform second-factor authentication for a given user account, users must do the following:

1. Send an email to support@collaborativedrug.com and cc the Vault administrator(s).
2. Include the new number, country if outside the USA, and the type (landline or mobile device).
3. The Vault administrator must approve the request.
4. Once approved, the number will be added to the user account and CDD will notify the user that it is available.
5. The user can then choose which number to use for their second-level of authentication.

Missing Phone Incident Response Procedure

If a phone is stolen or lost, the user must:

1. Immediately notify support@collaborativedrug.com and cc the Vault administrator(s).
2. CDD will disable access.
3. Once a new phone is established, the user must confirm that the existing number is now tied to a new phone or they must submit a new number. The Vault Administrator(s) must be included on and must approve this request
4. Once approved, CDD will make the changes and will notify the user once their account is activated.