AFR Account Management Best Practices

N·R·D™
National Registration Database

You are receiving this letter in your role as the Chief Authorized Firm Representative (CAFR) for your firm in the National Registration Database (NRD).

As you are aware, NRD contains sensitive information. The security of the data contained in NRD is paramount. The Canadian Securities Administrators (CSA) conducts regular reviews of the NRD to ensure that necessary protections and controls are in place to safeguard the data. The CSA also uses industry-recognized security services to monitor and protect the NRD and the data contained in the NRD from malicious activity.

Despite the safeguards in place at the system level, the failure of a firm to adequately manage its users' access to the NRD can lead to the unauthorized modification, destruction, or disclosure of the Firm's sensitive information contained in the NRD.

The enclosed Authorized Firm Representative (AFR) Account Management Best Practices Checklist has been prepared by the CSA based on ISO 27002 best practices for information technology. Although firms are expected to have their own security policies and procedures already in place, the CSA recommends that firms review their existing internal processes and controls against these best practices.

For more information, please refer to the FAQs below or contact your principal regulator or self-regulatory organization (SRO). You can find the regulator's contact information by visiting the NRD information website at www.nrd-info.ca.

Frequently Asked Questions (FAQs)

What is the risk? Why is managing access rights important?
As the NRD collects sensitive information, failure to adequately manage access rights can lead to unauthorized modification, destruction, or disclosure of that information.

Who can access NRD?
In addition to the securities regulatory authorities, a firm's AFRs and individual registrants may access and use the NRD website.

Who can see the registration information of a firm or an individual in the NRD?
Only the securities regulatory authorities and the AFRs of a firm have access to the NRD and can see the registration information. The AFRs have access to the registration information of their firm(s) and actively registered individuals only. Individual registrants may see their initial registration forms if they are granted permission to complete that form for the AFR to submit.

What are some best practices?
We recommend each firm verify the user identity when setting up a user's access, review the user's access on a regular basis with the List AFRs Report, and revoke the user's access immediately when access is no longer required.

Can the AFR user access be shared within the firm?
Sharing user access is not allowed. The CSA is committed to improving security on CSA IT systems, including user access security.

AFR Account Management Best Practices - Checklist

N·R·D™
National Registration Database

A Chief Authorized Firm Representative (Chief AFR) can set up other individuals to have access to NRD on behalf of the firm. Additional AFRs will either be:

- an Authorized Firm Representative (AFR), or
- an Authorized Firm Representative Administrator (AFR Administrator).

A firm will have only one Chief AFR, but it can have an unlimited number of AFRs and AFR Administrators. Because all AFR users can access the information in NRD, submit filings and authorize fee payments from the firm's bank account, it is important to have some controls in place to limit or audit user activity. Here are some best practices you can follow to manage your AFR users.

Setup User Access

☐ Review the user set up request with approvals by an authorized signatory.
☐ Verify whether the user has a legitimate business reason for the request.

Review User Access

☐ Conduct quarterly reviews with the List AFRs report to ensure only those who need access to NRD have access to NRD.
☐ Review account and role with users upon notification of job changes (e.g. termination, change in role).
☐ Keep the user information updated (e.g., the email and the phone number of the user).

Revoke User Access

☐ Revoke user accounts that are suspected or found to be no longer required.
☐ Revoke user accounts immediately upon a change in role where access to NRD is no longer necessary, or upon termination of employment.

Common User Access Guidelines

☐ Do not allow users to share accounts.
☐ Never share account passwords or store them in a plain text file.
☐ Only provide users the privileges needed for them to perform their jobs.
☐ Only provide one user account per user.