OUR RECOMMENDED SECURITY BEST PRACTICES

There are many security features of CEIPAL that aid in keeping your data private and secure. However, they won't work unless you configure them!

Below are our recommendations for adding extra layers of security to your CEIPAL account.

Password Policy

We strongly recommend configuring the system to accept complex passwords as it exponentially increases login security. Administrators have the ability to configure password requirements including setting a minimum length, requiring special characters, disabling accounts after a set number of invalid attempts, and setting the number of days a password is valid for before it needs to be updated.

One Time Password (OTP)

Have a question for a support representative? Don't just give them your password, utilize the systems' One Time Password feature instead. The OTP shared with the representative is randomly generated and expires a couple of hours after generation, thus keeping account passwords private. While our representatives would never misuse your data in the process of helping you, it helps get all users accustomed to using this security-enhancing feature.

2-Step Verification

Reduce fraudulent login attempts by enabling 2-step verification for all your users. Once enabled, the system requires users to enter both their password and a temporary, randomly generated code sent to their mobile phone number. Codes refresh every 30 seconds and, by combining something only users know (their password) with something only they possess (their phone number), there is a significant reduction in unauthorized access.

IP Restriction

Ensure only authorized users are getting into CEIPAL with IP-based access restrictions. Administrators can configure the system to be accessed from certain IPs and, if the IP is not whitelisted, the system will not allow access from that address. This ensures all users will be accessing the platform from trusted, known IP addresses to avoid potential misuse and instantly blocks anyone trying to remotely access company-sensitive files.

Updated November 2019