Database Security

Database Management · https://learning.pcrecruiter.net/site/docs/database-management/database-security/

In addition to the User Security settings, the system also offers database-wide security options.

1. Open **System** in the Main Menu
2. Select **Database Maintenance** from the submenu
3. Open **Security Settings**

Within this panel are three areas to configure.

Restrictions

User Security Level

- **Global Level Security:** Default, unrestricted behavior.
- **User Level Security:** Users can only see records bearing their own USERNAME. This applies broadly and can prevent users from seeing candidates, form letters, etc. Use with caution.
- **Record Level Security:** This setting locks the user out of Positions that do not belong to their account. All other content remains visible.

Allow / Whitelist IP Addresses

- **Allow only these IP addresses:** List IPs or ranges (append '/24' for a Class C subnet) one per line. Anyone attempting to log in from any non-listed IP will be blocked (regardless of system administrator status). This is recommended if you are storing sensitive data such as government identifications, banking details, or other critical info in your database. **Be sure to add your own IP to the list.**
- **Whitelist these IP addresses:** PCR will automatically log you out if your IP address changes. If your public IP address changes on a regular basis, add the possible addresses to this list to allow hopping between them without losing the session. After the IP address, append '/24' for a Class C subnet. The whitelist takes precedence over the 'Allow only' list.

Password

This panel defines the parameters for 'Strong Password' creation, automatic expiration of passwords, and so on:

- Require strong passwords
  - Require Symbol
  - Require Letter
  - Require Number
  - Require Upper Case Letter
- Allow only secure connections (HTTPS)
- Maximum Failed Logon Attempts
- Minimum Password Length
- Password to expire (default for new users)
- Maximum password age - in days
- Warn before expiring - in days (-1 for never)
- Allow Password to be re-used
- Days before password re-use (-1 for unlimited)

Encryption

[This feature is deprecated - for encrypted fields, see Encryption Security.]