Level 0 Security Levels

Descriptions and Samples
Level 0 Security Level: DDC/CIO

- DDC/CIO security level provides user with:
  - Read, Write, Lock and Upload access for authorized data types (student or staff).
    - If student data is authorized, DDC has Upload access to all student data including L0 Express.
    - If HR staff data is authorized, DDC has Upload access to only datasets indicated on the WNYRIC security form.
  - Administrative access to set up security for additional users within DDC’s authorized data types (student or staff).
- DDC/CIO level access should be limited to one to two people per organization, ideally one person for student data and one for HR data or the same person for both.
- DDC/CIO Level 0 security is set up by WNYRIC upon receipt of a Level 0 Security Form for DDC Level Access.
  - Two forms are available on the WNYRIC Forms Library.
  - One is for student data; the other is for HR data.
Level 0 Security Level: District User

• District User (Student or HR) access to Level 0 is more restrictive:
  – It does not provide administrative access for establishing security.
  – Access can be restricted by entitlement level:
    • Read: View only access.
    • Write: Can view and input data but cannot lock or upload.
    • Lock: Can Read, Write and Lock Data but cannot upload. It is not used for WNYRIC districts. Use Upload.
    • Upload: Includes Read, Write, Lock and Upload.
    • Note: To assign Upload for program data, “Allow FRPL Access” must be checked.
  – Access can also be restricted to certain data sets within data type (e.g., demographic, enrollment).
• Security is established within the organization by a user with the security level of a DDC/CIO.
Sample User Security Levels

1. Can set up users with access to student data; has HR access but can’t set up HR users.
2. Can set up both student and HR users.
3. Can set up student users. Has no access to HR data.
4. Has no access to student data. Can set up HR users.
5. Has access to both student data and HR staff data. Cannot set up users at all.
Adding a District User

By User with DDC/CIO Security Level
DDC/CIO: Step 1. Adding a new District User

- Enter user name, user ID (e.g. first initial and last name), click auto-generate and a temporary password is generated.
- Enter work e-mail, click on district and click Save User Permission.

![User permission setup interface]
DDC/CIO: Step 2. Adding a new District User

• Once user name is saved, select District User for Student Security Level or HR Security Level or both.
• Select entitlement level (e.g., Upload) for the desired data sets (e.g., demo) and click Save User Permissions.
• Notify user of user ID and password. User will be prompted to change password on initial login.
DDC/CIO: “Allow FRPL Access”

- Check “Allow FRPL Access” if Upload is selected for Program Fact.
Periodic Review of Level 0 Users in Your Organization

“View All Users”
Periodic Review of Level 0 Users

- Click on “View My Users”.
- Review Student and HR access levels, entitlements, and login information.

![User Access Management Interface]

Entitlement Key: R = Read, W = Write, L = Lock, U = Upload and Blank = no access.
(Note: If ‘+’ with Program Fact, FRPL access allowed. If ‘+’ next to RIC_Staff, user setup access allowed.)

My Entitled Level 0 Users: (District Filter: SNOWY TOWN)

<table>
<thead>
<tr>
<th>User Name</th>
<th>User District</th>
<th>Student</th>
<th>HR</th>
</tr>
</thead>
<tbody>
<tr>
<td>District User</td>
<td>SNOWY TOWN</td>
<td>District_User</td>
<td>U U+ U U U U U U U U U U U</td>
</tr>
<tr>
<td>Dory Fish</td>
<td>SNOWY TOWN</td>
<td>District_CIO</td>
<td>U U U U U U</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Log In</th>
<th>Log Ins Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/8/2016</td>
<td>40</td>
</tr>
<tr>
<td>6/22/2016</td>
<td>1</td>
</tr>
</tbody>
</table>
Periodic Review of Level 0 Users

• Change entitlement levels (e.g., Read, Write, Upload) and data sets (e.g., demo, enrollment) within your authorization level as needed.

• Send request to dataview@e1b.org to:
  – Delete an existing Level 0 user.
  – Change the security level from District CIO to District User

• If you have questions, e-mail dataview@e1b.org.