

iGroup Security Model

Roles and Responsibilities

BCeSIS Project Team

- Provide secure authentication system.

BCeSIS iGroup

- Create User accounts.
- Reset User accounts.
- Setup User security levels.
- Manage user accounts for trainers and helpdesk support staff.

BCeSIS Independent Schools

- Have separate username for each user of the system
- Ensure that accounts are minimal in access levels. (i.e. users only have access to what they need, not what they want)
- Supply primary and alternative security contact, with permission to request username creation and reset.
- Ensure that user accounts are removed when staff leave school.

User Definitions

BCeSIS iGroup District Manager

Manager of district 200 and is responsible for user account management, district level configuration, and conversion into Stage 1. This person should have access to all forms, reports, and screens in BCeSIS for district 200. This person should be the only one with access to create user accounts or change account permissions. Furthermore this person should be the only one with access to change the district level configuration.

BCeSIS iGroup Helpdesk.

Responsible for responding to helpdesk support requests. (You can't say this, because further down, you say they **will** have access through remote access software.). They will have read only access to district level settings. These people will have access to the training DB for testing solutions. Using remote access software and permission from school project managers they will have access school level information, on a temporary basis and only for the purpose of solving users problems. (Remote access software requirements and specifications outlined in Level 1 Support strategy)

School BCeSIS administrators.

Primary operators of BCeSIS in their school. They are responsible for setting up the school, timetables, student admissions and withdrawals and for the administration of students in their school (i.e. course registration, meeting graduation requirements, etc). They have access to all forms and reports at the school level and school configuration.

School Secretaries.

Primarily responsible for reporting student activities in schools e.g. attendance, grades. They will have access to all student information in their schools. They will not have access to admit or withdraw a student, change school configuration or view incident

reports. (This might not be true in all schools, I think the school secretaries might do a whole lot more than out lined here.)

School Principals.

Primarily responsible for the day to day operations of education in the school. As such these people will have read only access to all forms and reports.. However they will have write access to incidents, and to withdraw a student. They cannot change school configuration.

School Teachers.

Teachers are responsible for the education of the students in their classes. They will have access to all information on students in their class. They will be able to take attendance, input grades. They will not have access to change information on a student (i.e. Name, address, phone number), or access to incident information.

Additional User Security Levels.

Admission, Withdraw and Cross enrollment of students.

This role allows a user to admit, withdraw, register and cross enrol students.

Attendance

This role provides access to run daily attendance reports as well as update access to the autodial valet extract, update access to daily attendance screens, run period attendance reports, update access to period attendance screens.

Course Maintenance

This role gives a user access to update course maintenance and course section maintenance for scheduling purposes.

Discipline / Incidents.

This role gives a user access to update student incidents.

General School Reports.

This role gives a user access to run General School Reports such as student program assign, the General Data Extract, 1701, Student Index and Course Credit information.

Scheduling

This role gives a user the ability to run daily attendance reports, update student course selections, and view student demographics, parent information emergency contacts and the student diploma, it also gives a user access to run schedule-building reports.

Security Model.

See Security Roles Details Document on Website

Processes for Security

Process for User Creation.

1. Determine who will use the system
2. Determine how each user will use the system.
3. Review the iGroup's user definition and model
4. Determine which of the user types each of your users most closely matches.
5. Determine any additional user access levels required.
6. Login to BCeSIS iGroup Security Center and create usernames.

Process for Start of new school year.

1. Determine any change of roles in your school.
2. Determine what access levels need to be added or removed for each user who has changed roles.
3. Update security levels in BCeSIS iGroup Security Center
4. Determine any users who have left your school.
5. Delete usernames from BCeSIS iGroup Security Center
6. Determine any users who have joined your school
7. Create users in Security Center (see process above)
8. Typically updates take a few hours.

Process for Password reset / Username deletion.

1. Determine the username of the person to be deleted or password reset.
2. Person with the authority to reset/delete usernames logs into Security Center and resets passwords
3. Typically username resets take a few hours.

Process for Changes to User Security Levels

1. Determine the user that needs a change to security level
2. Determine what security level needs to be added or removed.
4. Person with the authority to reset/delete usernames logs into Security Center and updates security levels
5. Typically username updates take a few hours.
3. Review usernames new security level to determine if need to meet

Change Management for Security Roles.

1. Determine the change that is required, and what roles it will affect. Provide rationale for the change, and why it cannot be done using the existing model.
2. Submit change to the BCeSIS iGroup Project Manager.
3. Project Manager will determine if change can be done using the existing model.
4. If can be done, inform user of this possibilities, check if meets users requirements.
5. If cannot be done, then determine the impact of the change on the current users.

6. Notify the current users whom it will impact.
7. Get approval from the BCeSIS iGroup Executive to make the change.
8. Submit issue to BCeSIS Security Working Group Committee.
9. If rejected, Project Manager will determine next course of action (resubmit modified version, or inform user that it is not possible)
10. If approved, plan for changes in the district.
11. Apply new security roles.