Conductor Security White Paper

1. Application Security

a. Encryption
   i. The system supports standard HTTP connection or encrypted connection (HTTPS) – SSL via any provider, Learn-Net recommends VeriSign.
   ii. It is recommended to use SSL at least for the login page.

b. User and Password
   i. The application can only be accessed by a valid user name and password.
   ii. In the case of a wrong user/password entry, the error message does not give the user any information about what's wrong, only that the user and password are incorrect (or if the user is suspended).
   iii. Password must contain letters and digits.
   iv. Password must be longer than five characters.
   v. Password must be changed any "N" days.
   vi. New password must be different than the last two passwords.
   vii. Password change history is recorded.
   viii. Three mistakes while typing user/password blocks the user.
   ix. The administrator can suspend a user (and record the reason for it).
   x. The system supports biometrical, physical (such as smart cards) and third party (such as passport) authentication.
   xi. There is no direct access to any of the application pages or forms.
   xii. The application logon form can be replaced
   xiii. The user name and password are stored in the different entities (student, teacher, staff, etc) record. The authentication is done using a one view on those tables. This view can point to different tables or be replaced by a physical table that will be managed by another application.
   xiv. The system can interface LDAP such as Active Directory. It can be done in two ways:
      1. The Active directory is the controlling application; in this case the logon form has to be modified to access the active directory.
      2. The Active directory is the slave; in this case the recommended method to update the active directory is via database triggers.

c. Log

i. All entrances and exists are logged.
ii. The system logs any data inserts, updates and deletions.

d. Deletions
   i. No physical deletion to any of the important entities such as a student, teacher, etc. is permitted.
   ii. No deletion or update to financial data is permitted, only "storno" changes.

e. Permissions
   i. The system uses user templates to manage permissions, any user must belong to a template
   ii. The system supports all three user types: staff, teachers and students (parent is equal to a student)
   iii. The system has a multi-dimensional security model:
      1. Forms a user access (and what a user may do with each form – No access / View only / Edit) are defined by the user template.
      2. Information that will be displayed on each form for the specific user – This is defined via the organizational tree.
      3. Role based permissions – A section/study group/teacher automatically sees their students, a class/homeroom teacher can see all their students.
      4. User type based permissions – Each one of the four user types (administrator, staff member, teacher and student) have a predefined permissions:
         a. Students can see all the data about themselves and change only their address and phone number.
         b. Students can see pre-defined information about courses, study/groups/sections, curricula, timetable, etc.
         c. Teachers can see all the data about themselves and change only address and phone; they can see specific data about their students, classes, study groups and can update evaluation events, grades, attendance and disciplinary events.
         d. Teachers can see pre-defined information about courses, study/groups/sections, curricula, timetable, etc.
         e. The template and the organizational tree define a Staff member's access.
         f. A Teacher can be a staff member.
         g. The Administrator can see it all.
         h. The basic student and teacher templates can be modified.

iv. The system enables the creation of a specific menu for each template.
v. The system enables setting permission on any form for a specific template. Permission can be an edit, view only and disable.
vi. There are two staff member user levels: standard user and supervisor.
vii. Every user belongs to a position on the organizational tree/chart, which represents their hierarchy in the organization (Example: The Lower School Principal will be positioned at the schools level of the organizational tree). A user can see information based on his position in the organizational tree.
viii. A second tree level can be assigned to a user. This level is “View only” (Example: the Assistant Head of School who is in charge of curriculum will be positioned in his first tree level at the school's management tree level that is bellow the school root level, but his second tree level will be the school root allowing him to see all students).

f. Misc.
   i. The application is using cookies only for the session id (as a session cookie). No data is stored in cookies.
   ii. The user's session is stored in the database.
   iii. The system has an automatic logout if the user hasn't touched the keyboard 'N' minutes.

2. Network Security

a. The application supports any server/network security policy such as VPN, IPSec tunneling.
b. The application supports an N-Tier solution where the web server, application server, and the database server can run on different machines. We highly recommend separation of the database server from a combined application + web server.
c. Protocol transformation can be used between the web server and the database server. It can be used as a different TCP/IP port or a different protocol such as named pipes (a non routable protocol).
d. There is no access by the users to any physical disk on the server.
e. The application uses only HTTP, HTTPS ports over TCP/IP protocol.
f. The application supports any firewall.
g. The application supports proxy and reverse proxy.
h. FCS may require special configurations.

3. Database Security

a. The application uses a two-phase login where the user logs in to the application and the application logs on to the database (with a different user name and password).
b. The application supports any security definitions made on the database side.
c. The connection to the database is done in OLEDB and not ODBC/JDBC. OLEDB/native providers do .Net applications.
d. The connection string is stored in a UDL file. This file is located outside the scope of the web server root or virtual directories.
e. Database communication can be encrypted using database client or third party application.
f. The portal & e-learning module can be installed on a different web server and different database server.
g. All access to the database is encoded (A user cannot type a problematic characters such as ' and ""). Although we use dynamic SQL, we encode the user's input to prevent SQL injection.