Aspen Security Strategy Statement

SECURITY STRATEGY

We built Aspen to include security as a core component of the design. This design includes a strict adherence to the separation of different layers within the application. Users interact with a presentation layer that is strictly HTML. All business logic operates on the application server in a business layer that is isolated from both the presentation and the database access. Finally, all database access is handled by a third and isolated persistence layer. Thus, between the end user and the actual storage of sensitive data, there are three independent layers in the Aspen application that all play important roles in ensuring only the appropriate data gets to the each user.

Our approach to security at the design level means that typical hacking techniques such as SQL injection and Cross-Site Scripting (XSS) are blocked—not by patches and fixes to vulnerabilities that come out on a periodic basis, but by the basic design of the application and encapsulation of each layer.

Aspen provides system administrators with security tools to limit user access to specific data elements, down to the field-level, and specific schools to ensure each person in the district has all of the information they need and none they don't. Users do not see the items they cannot access. These tools allow districts to create a security policy that is FERPA, HIPAA, and CIPA compliant.

SECURITY ARCHITECTURE

User Account Structure

Each user in Aspen is given one user account that will determine their access to appropriate functionality in the system. In Aspen, there is no need to have different user account for users who cover multiple areas of functionality (for instance, a parent who is also a teacher.) User IDs can be determined by the district. The traditional login ID is "first initial last name" (e.g. jsmith), but Aspen allows for login IDs that combine any element of the person record (e.g ID number, phone number, etc.)

Aspen provides the following options for configuring the district's password policy:

- Days before expiration
- Minimum length
- Require digits
- Require mixed case
- Require non-alphanumeric characters
- Pass heuristic tests (for example, password cannot be user's DOB)
- Unique number of passwords before user can recycle old value
- Number of invalid attempts before an account is disabled

Aspen does not store plain text passwords in the database – all values are encrypted using a one-way hash function. Passwords can also be reset for individual users or multiple accounts at once. Aspen alerts users to change their password on the day it expires.

Password Recovery

Self-serve

Users that forget their password can either use the self-service password recovery feature or contact an administrator to reset the password. Passwords can be reset for individual users on a case-by-case basis or en masse for groups of users. Aspen is capable of automatically resetting a user's password. On the login page, users can click on the "I forgot my password link" and, if the correct e-mail address and security question response are entered, an e-mail is sent containing a new password. The user is prompted to change this password on their first login. Users must have a valid e-mail address and security question response in the system in order to use this feature. This information can be entered on the Security tab in the Set Preferences popup window. The system can also be configured to automatically prompt for this information immediately after login.

System Administrator

Users with the appropriate privileges can also reset another user's password and login as that individual. Once the problem has been resolved the password can be set to require changing upon next login.

System Usage

Aspen allows system administrators to view the list of active sessions for the system. This list includes the user's name, originating IP address, current location in the system, login time, and last access time. Sessions can be terminated (i.e., remotely logging the user out of the system).

User Account and Profile Maintenance

Aspen includes a Create User Accounts wizard that creates users accounts and the associated security roles for a group of staff members, students or contacts. The group can be based on the results of a query or an ad hoc selection. Once created, user accounts are managed via a master list in the District view. Accounts can be disabled, set to expire on a specific date, or be restricted to access the system from a specific subnet of IP addresses.

Randomly-generated, strong password can be generated for each user account. Letters or labels can then be printed with the login ID and temporary password for each account. Users will be prompted to change the password upon first entry.

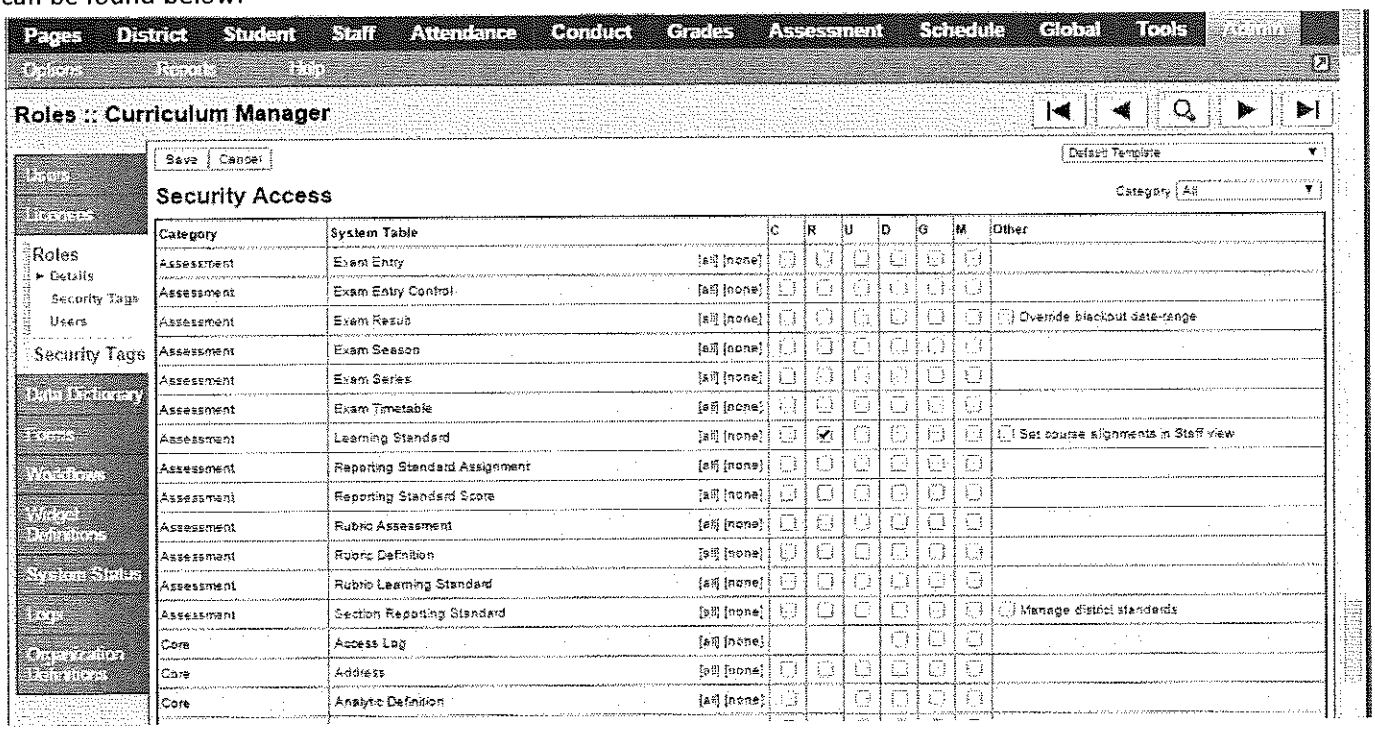
User Group Profile and Maintenance

Aspen provides role-based security. Roles are defined and granted privileges to create, read, update, delete, or mass-update (CRUD-M) records in a particular table. There are also business privileges for special operations like archiving a student or accessing teachers' grade books. Roles are then assigned to users. Aspen allows users to be associated with multiple roles and with multiple schools. A user gets the cumulative privileges allowed by those roles.

Aspen also allows roles to restrict access to specific screens even if standard CRUD-M privileges would allow it. For example, a user may be allowed to access the attendance records for one student at a time but not be allowed to access attendance for all students at once (even though the application is reading from the same database table).

User and Group Access Security Matrix

Each user role created in Aspen allows the system administrators to define a "matrix" of access to both tables and fields, along with views (modules), menus and functions. A screen shot of the security matrix can be found below:



Audit Reporting of System and Application Access

Aspen has auditing abilities. Aspen includes an audit trail component that can be enabled for any table and field in the Data Dictionary. For each record modified, the audit trail shows who made the change, what was changed (both the original and new values), and when the change was made. Aspen includes all its core query, sorting, and reporting tools with the audit trail feature.

Aspen allows users with the appropriate privileges to view a record's audit trail history from within the application. Aspen makes use of security roles to restrict users from intentionally deleting data, alerts and prompts to prevent users from accidentally deleting data, and the audit trail to record what data may have been lost.

MANAGING SECURITY

Aspen has over twenty predefined roles that can be modified, copied, or deleted to suit the needs of your district. Security roles and user accounts are grouped in an area of the application that, by default, is only accessible to users with the System Administrator role. Through the use of security roles, a system administrator can determine exactly what data elements a role can access. The maintenance of these user accounts and roles is controlled centrally and users can be given the ability to perform certain security administration functions (e.g., create and update an individual user's security profile, reset passwords, etc.).

FOLLETT DATA CENTER

The Follett Data Center contains approximately 6,000 square feet of raised floor space. The data center was designed to reduce or eliminate as many single points of failure as possible.

- There is a dedicated 500Kw generator for the data center. In the event there is a need for extended maintenance on the generator, there is a connection to the transfer switch for a portable generator.
- There are two uninterruptible power system (UPS) units for the data center. If we incur a failure on one UPS unit, the full load is switched to the other unit.
- There are two electrical paths from the automated transfer switch to the server in the rack. Again, any loss of power along this path will result in the load shifting to the other path.
- There are two fire suppression systems in the data center. If the FM-200 system does not extinguish the fire, there is a dry-pipe system that will provide a localized fire sprinkler to put out the fire.
- The cooling system for the data center has been sized to provide an extra HVAC unit in the event there is a failure of any one unit. There are currently four 20 Ton HVAC units in the data center.
- There are two network access points to the data center from the street.
- The raised floor space sits on a 24" plenum. Only electric power distribution is delivered from below the floor.
- The data network is provisioned from a cable ladder and cable tray system suspended from the ceiling.

Physical access to the data center is controlled by a card proximity reader. Only individuals with a role that requires access to the data center are permitted in the raised floor area. Access to the mechanical space is similarly controlled. A camera system has been installed at the doors to the data center to record entrance and exit to the raised floor and mechanical space. Procedures are in place to log the access to the data center.

Follett Data Security

Follett is committed to data security and supporting our customers' data privacy needs. As student data collection evolves, it is important to review how Follett continues to provide the necessary levels of security for your information systems.

Aspen

Aspen provides several levels of security that control access to your student information system from people external to your organization, internal to your organization, and even among other Follett products that you are using.

Aspen was architected with security in mind

The Aspen data model consists of a single database, meaning that data does not need to be replicated to other data stores. Security rules are applied universally to each database instance when it is created, and the database is not accessible from outside the data center firewall. Each Aspen customer has a separate logical database, and each Aspen instance only has the user account of the database for that instance.

Security and penetration tests are routinely run on Aspen to verify that our security is intact; in fact, it's a contractual requirement for some of our customers. This testing allows us to verify that the security measures we've developed—such as the cross-site scripting protection layer that prevents database access via SQL injection—are working to prevent known attack vectors.

Aspen has multiple levels of data security

All access to the database is managed through the application, and the data is only visible to users with specific rights and permissions. You can apply your data security in a number of ways:

- **Field-level security**—Security can be applied to individual fields of data. For example, some customers store student social security numbers in Aspen. Access to the data in this field can be locked down while allowing a teacher to see the rest of the data associated with this student.
- **Entity or component-level security**—Security can be applied to whole components of the system. For example, you can allow access to "Transcripts" but not "Conduct."
- **Record-level or scoping security**—Teachers can only access records for students that they are currently teaching.
- **Navigation security**—Access to entire areas of the system can be controlled by disabling tabs and sub-menus in the system.
- **User Interface security**—Requests cannot be manipulated to try to gain access to data that the user does not have permission to view.

Aspen has over twenty predefined user roles that can be modified, copied, or deleted to suit the needs of your district. Through the use of security roles, a system administrator can determine exactly what

data elements a role can access. Security roles and user accounts are grouped in an area of the application that, by default, is only accessible to users with the System Administrator role. The maintenance of these user accounts and roles is controlled centrally and supports any user policies you decide to enact.

Aspen has auditing abilities that allow you to review and confirm that your policies are working the way you intended. Aspen includes an audit trail component that can be enabled for any table and field in the Data Dictionary. For each record modified, the audit trail shows who made the change, what was changed (both the original and new values), and when the change was made. Only users with the appropriate privileges to view a record's audit trail history can do so. Aspen also makes use of security roles to restrict users from intentionally deleting data, alerts and prompts to prevent users from accidentally deleting data, and the audit trail to record what data may have been lost.

Aspen complies with FERPA guidelines

The Family Educational Rights and Privacy Act (FERPA) business rules are built into system so that guidelines (for example, teachers can only access student data for students that they teach) is automatically enforced. System-wide searches only show directory info that is within the FERPA guidelines. The comparable Canadian privacy act, Freedom of Information and Protection of Privacy Act (FOIPPA), is currently in development for the next release of the Aspen software.

Student-identifiable information is not shared or uploaded to any other systems from Aspen—including other Follett Software Solutions such as Destiny, One Search, WebPath Express, State Standards, or any content delivered through a Digital Content Provider Integration.

Destiny

Destiny shares many of the same security attributes as Aspen.

- The data model consists of a single database; data does not need to be replicated to other data stores.
- Each Destiny district has a separate physical database file.
- Security rules are applied universally to each database instance.
- The database is not accessible from outside the data center firewall.
- All access to the database is managed through the application, and data is only visible to users with specific rights and permissions.
- Destiny is routinely tested against attacks using automated acceptance testing, such as exercises and sample data intended to uncover SQL injection vulnerabilities. Authentication methods are exercised through automated unit tests to validate that data access is restricted to users with the appropriate permissions.

Destiny has multiple levels of data security:

- **Session-level authentication**—All data access within Destiny is routed through a layer that checks authentication credentials and permissions on each request.

- **User Interface security**—The Destiny interface presents different options based on the permissions associated with the users.

Follett Shelf

Follett Shelf uses a slightly different data model consisting of a clustered database where all Follett Shelf customers share the same database. All user data is stored in the database; Follett Shelf only stores the username, password, first name, and last name for students and teachers. (Follett Shelf optionally stores the email address for site administrators.)

Follett Shelf has the following security attributes:

- Security rules are applied universally to each database instance.
- The database is not accessible from outside the data center firewall.
- Security and penetration tests are routinely run; automated tests run nightly to validate quality.
- Follett Shelf import/export data is stored on the application layer.
- All access to the database is managed through the application, and data is only visible to users with specific rights and permissions.

About Our Data Center

The Follett Data Center is an approximately 6,000 square-foot, raised-floor facility. Physical access to the data center is controlled by a card proximity reader. Only individuals with a role that requires access to the data center are permitted in the raised floor area. Access to the mechanical space is similarly controlled. A camera system has been installed at the doors to the data center to record entrance and exit to the raised floor and mechanical space. Procedures are in place to log the access to the data center.

Contact Us

Follett is committed to helping our customers demonstrate the privacy and security of their student data. Our security features are designed to provide physical and digital security and empower districts to develop, enact, and enforce their privacy policies. For more information about our data security, please contact us.

Original Invoice

X2 Development Corp
a Follett School Solutions Company

Follett

Page	1
Invoice#	16804
Invoice Date	JUL 02, 2014
Sales Order#	5000433
Customer#	2027019
Customer	DUXBURY PUB SCHS

Bill To:
ATTN: ACCOUNTS PAYABLE
DUXBURY PUB SCHS
130 SAINT GEORGE ST
DUXBURY MA 02332

Ship To:
DUXBURY PUB SCHS
130 SAINT GEORGE ST
DUXBURY MA 02332

Purchase Order	Sales Representative	Follett Contact	Shipping Date
Aspen Renewal			
Due Date	**Terms**	**Tax ID#**	**Shipping Information**
AUG 01, 2014	NET 30-SH	14-1853680	-

Summary

Send Payment To
X2 DEVELOPMENT CORPORATION
62084 COLLECTION CENTER DR
CHICAGO, IL 60693-0620

Billed & Payable in USD

	Billed & Payable in USD
Sub Total	$40,140.00
Tax	$2,433.74
Invoice Total	**$42,573.74**
Payments & Credits	-$2,433.74
Outstanding Balance	$40,140.00
Amount Due as of JUL 07, 2014	**$40,140.00**

Payment/Credit Details

Due Date		Payment
JUL 03, 2014	Adjustment - Tax	-$2,433.74

Details

Item Number / Description		Quantity	Unit Price	Ext Price	Tax
95204P	DUXBURY PUB SCHS **Pupil Cnt 3245** ASPEN CURRICULUM AND LEARNING - DISTRICT - SAAS: JUL 01, 2014 - JUN 30, 2015	1	6,490.00	$6,490.00	$405.62
95722P	DUXBURY PUB SCHS ASPEN ONLINE PROF LEARNING PER CONNECTION: JUL 01, 2014 - JUN 30, 2015	1	1,200.00	$1,200.00	$0.00
95201P	DUXBURY PUB SCHS **Pupil Cnt 3245** ASPEN STUDENT INFORMATION: JUL 01, 2014 - JUN 30, 2015	1	25,960.00	$25,960.00	$1,622.50
95550P	DUXBURY PUB SCHS **Pupil Cnt 3245** FOLLETT HOSTING: JUL 01, 2014 - JUN 30, 2015	1	6,490.00	$6,490.00	$405.62

End of Invoice