Altum

Nurturing What's Possible

12100 Sunset Hills Road, Suite 101, Reston, VA 20190 | p +1 877 GO ALTUM f +1 703 964 5939 | altum.com

proposalCENTRAL Security Questions and Responses

1. What is Altum's approach to security for proposalCENTRAL?

Altum has incorporated security at each level of our operation – physical site security, router, firewall, operating systems, applications, and databases. The following describe the primary security precautions that Altum provides:

A. **Physical Security.** Altum servers are hosted at a commercial ISP (Level 3 in McLean, VA) - an off-site location, separate from its business offices, and are accessible only by designated Altum employees. This data center site is monitored by video surveillance and monitored 24-hours a day. Access to the servers is by key card, biometrics and combination locking cabinets within the data center. At our business offices, Altum uses independent key access systems to control access to our facilities. These site security systems ensure that only authorized employees have access to its facilities and only access to areas for which they have been authorized.

B. **Firewall.** Altum utilizes a well-known, reliable, and extremely secure firewall, stateful failover solution from OpenBSD and PF (Packet Filter) to protect proposalCENTRAL, its network, applications and customer data from unauthorized external access.

C. **Secure Sockets Layer.** Users connect to proposalCENTRAL with the industry standard SSL (Secure Sockets Layer) encryption capability of their web browser. SSL encrypts the user's private information and transmits it securely via the Internet to proposalCENTRAL. When accessing proposalCENTRAL, users can verify that the secure SSL connection is in use through the URL web address which changes from "http:" to "https:" and by the appearance of a closed lock or key symbol at the bottom left of their browser window.

D. **Authentication.** Each proposalCENTRAL user is authenticated with a two-field (User Id and password) authentication system. Each individual attempting to log in must provide a User ID and a Password before gaining access. The log-in session is SSL encrypted.

E. **Automatic Idle Session Time-Out.** User sessions that have been idle for more than 10 hours are automatically terminated.

F. **Authorization.** Each User is assigned a security profile that determines which modules, features, and objects can be accessed and which documents can be modified. Security profiles are set-up at the community level for multi-project access rights, and at the project level, for the safeguarding of information within specific projects.

G. **Application and Data Security.** The proposalCENTRAL application architecture is comprised of an application layer written and managed in Microsoft .ASP, Microsoft Windows Server operating system, IIS web server, and MS SQL database server. Database access is managed and controlled at the application, operating system and database connection levels.

H. **Virus Protection.** All documents submitted by Users to proposalCENTRAL are scanned for viruses continuously in real-time as they are submitted and prior to being stored in the proposalCENTRAL database. Altum's anti-virus software is automatically updated daily and more frequently if virus threat alerts are received. Altum technical support staff electronically monitor the top anti-virus web sites for new or potential virus threats and are automatically alerted to changes on these web sites.

2. How is physical access to the proposalCENTRAL servers and their associated data protected?

The physical structure of the Level3 data center is a brick building and has no external windows; it was a former CIA building and purchased by Level3 for its sound structure and security. There is a single door for entrance which is protected by a card reader. Photo RFID access cards are only issued to authorized Altum employees; currently the only members with physical access are:

A. The Chief Executive Officer, who is also the authorized badge administrator to revoke access if necessary.

B. The system operations team of system engineers so that they can attend to physical needs of the data center cabinets and servers.

After badge access is granted through a card scan at the front door, a biometric hand scan along with another card scan is necessary to enter the actual data center facility. Naturally the card used at this door must match the biometric scan.

When access is granted into the data center, Altum has two separate, locked, ventilated cabinets. The cabinets are locked with a 3-digit combination lock that is only known by the Altum executive team and the system operations team. The cabinet codes are kept in the master password KeePass database.

3. How does Altum keep unwanted users and malicious activity off its network?

In addition to the physical security provided in #2 above, remote access to servers is limited to Altum system administrators (by role and separate userid and password authentication). The remote access is controlled through SHH tunneling. T he SSH access logs are stored on Altum's syslog server and are monitored frequently for attempted breakins. If necessary (e.g., multiple break-in attempts or other malicious activity detected), Altum's system administrator will ban specific IP addresses.

4. How does Altum maintain data integrity within its databases assuring only authorized users have access?

Access to the proposalCENTRAL database, data and files is limited to two areas:

A. The proposalCENTRAL user screens (with the software's built in access restrictions and business rules).

B. Direct system and database access by Atum's system/database administrators and technical support personnel for application maintenance and testing.

Part A is addressed in the responses that follow.

For B, there are only a very limited number of Altum employees that have authorization as System or Database Administrators to the proposalCENTRAL (currently limited to 2 systems administrators and 1 database administrator). The Systems and Database Administrators are authenticated via a separate system userid and password (separate from the proposalCENTRAL user authentication). Two Quality Assurance Specialists have read only access to the database for testing and quality assurance, which does not allow them to make modifications to the data.

5. How does proposalCENTRAL restrict access to information? Application and Data Security.

The proposalCENTRAL application architecture is comprised of an application layer written and managed in Microsoft .ASP, Microsoft Windows Server operating system, IIS web server, and MS SQL database server. Database access is managed and controlled at the application level with specific restrictions, first by user authentication, then by user authorization to specific functions and associated data.

6. How is access by users of proposalCENTRAL restricted? Authentication.

Each proposalCENTRAL user is authenticated with a two-field (User Id and password) authentication system. Each individual attempting to log in must provide a User ID and a Password before gaining access. The log-in session is SSL encrypted.

7. How does proposalCENTRAL restrict users to specific functions and data. Authorization.

Each User is assigned a security profile that determines which modules, features, and objects can be accessed and which documents can be modified. Security profiles are set-up at the community level for multi-project access rights, and at the project level, for the safeguarding of information within specific projects.

A. Applicants – Access only to their applications and grants, can give access to others (like co-investigators, authorized organization officials).

B. Reviewers – Access only to the application and review data as allowed by the Program Administrators (grantmaker staff).

C. Program Administrators (e.g. grantmaker staff) –Program administrators have several levels of access control:

i. GrantMakerAdmin ("GM Admin") access allows program administrators to access their data (e.g., applications, reviews and awards, data and documents) in all proposalCENTRAL modules. GM Admins can give access to other program administrators and set their access permissions.

ii. Post Award Administrators - Program staff with full GM Admin access can grant various levels of access to users that need to access the proposalCENTRAL Post-Award Module. These levels of Post Award access are as follows:

a. Edit All -This permission will allow the user to access, edit, and perform actions for all awards in proposalCENTRAL. In addition they can add administrative users and configure their permissions as well.

b. Read-Only All- This permission will allow the user to access all awards, however only edit award information and perform actions for their assigned awards. In addition, this user would have access to the following pages: Add An Award Deliverable, Deliverable Setup, Outcomes Setup, Access and Assignment, Classification Keywords, and Import Payments.

c. Edit Assigned, Read-Only Unassigned (Admin)- This permission will allow the use to access all awards, however only edit award information and perform actions for their assigned awards. In addition, this use would have access to the following pages: Add an Award, Deliverable Setup, Outcomes Setup, Access and Assignment, Classification Keywords, and Import Payments.

d. Edit Assigned, Read-Only Unassigned (Staff)- This permission will allow the user to access all awards, however only edit award information and perform actions for their assigned awards. The user will not have access to the following pages: Add an Award, Deliverable Setup, Outcomes Setup, Access & Assignment, Classification Keywords, and Import Payments.

8. Who has access to an in-progress proposal?

Any user can start an application by accessing proposalCENTRAL through a secured web-browser (https) using their User Id and password. The user (i.e. applicant) is the only user with access to their application.

The applicant may allow other users of their choosing to have access to their application. Only the users the applicant granted access to will be able to see the applicant's application. In addition, the applicant may give the users they provided application access, specific permission levels:

A. View - View only; cannot change any details.

B. Edit - Can view and change information in the application. Cannot submit the application or grant others permissions to the application.

C. Administrator - Can view, edit and submit the application. Can also give access rights to others.

Altum's customer service representatives have access to all proposals (and other proposalCENTRAL information) in order to assist our clients and their users with questions. The Altum proposalCENTRAL staff members are required to keep all information confidential (by the proposalCENTRAL contract and via their employment agreement). Altum staff can sign additional non-disclosure agreements upon client request.

9. Who has access to a submitted proposal?

An applicant, and anyone else the applicant provided application access to, will still be able to see the application once it's submitted.

Grantmaker staff members with permissions of "Grantmaker Administrator" are the only ones who have access to all of the submitted applications for their organization. There are several other permission levels that can be granted by the Grantmaker to their own staff members or external parties (e.g. reviewers).

If a Grantmaker prefers to restrict access of applications for their internal staff members, they can assign the applications to different committees and add the appropriate staff member to the committee as a "Committee Administrator". This allows the internal staff member to see only the applications in their committee.

As part of the review process, Grantmakers also assign reviewers to committees. A reviewer can only see the applications assigned to their committees. In addition, the Grantmaker can choose if the reviewer only has access to the applications assigned to them for critique or if they have access to all applications in the committee. The Grantmaker sets this configuration and has the ability to change it during the process.

10. What information do reviewers have access to in proposalCENTRAL?

Each reviewer has their own User Id and password that authenticates them and restricts their access to that of a reviewer. Reviewer access is controlled committee by committee by grantmaker program administrators.

The Grantmaker configures in proposalCENTRAL what their reviewers can see. Access for reviewers can be configured in different ways in different committees to accomplish whatever levels of restricted access are required by the client.

The Grantmaker determines the access level for each committee for the following items in the Committee Settings:

A. If the reviewers can access only their assigned applications or all applications in the committee.

B. If the reviewers can see: no critiques, only co-reviewers critiques, all critiques in the committee, or all critiques from all committees their assigned application was in. (Note – In order to prevent biased critiques, even if a reviewer is allowed to see their co-reviewers critiques, they will never see those critiques until after they submitted their own critique.)

C. If reviewers are identified to each other by name or an anonymous reviewer role. (Note – Applicants never see reviewer names.)

D. If the reviewer can see the Over All Score for each application based on the committee's scoring and voting.

E. If the reviewer can see the Rank for each application based on the committee's scoring and voting.

F. If the reviewer can see the Average Score for each application based on the committee's scoring and voting.

G. If the reviewer can see the Average Score for each application based on all committees' scoring and voting (i.e. if applications were critiqued in multiple committees).

H. If reviewers can participate in an on-line threaded discussion. (Note – In order to prevent biased critiques, even if reviewers are allowed to participate in on-line threaded discussion, they can't do so for their assigned applications until their critique has been submitted.)

The Grantmaker can change the configuration to enable reviewers to see more (or less) information during various stages of the review process. For example, reviewers could be restricted to just their assigned applications and no other application or reviewers' critiques. During the review committee meeting, or earlier as appropriate, the reviewer's can be given additional access.

11. Who has access to the reviewer's comments/critiques/discussion/scoring?

The "Grantmaker Administrators" are the only users with access to all critiques for all committees. Within a particular committee, the following roles have access to all critiques for the committee regardless of the Committee Settings: Committee Administrator, Reviewer Plus, and Observer. Those roles are designated by the "Grantmaker Administrators" allowing them to elect who, if anyone, within a committee can see all the applications and critiques.

The users with a role of "Reviewer" within a committee only have access to the critiques as prescribed in the Committee Settings (described in #10 above).

The applicants can only see critique information if the Grantmaker elects for them to see it. In addition, the Grantmaker can modify the critique information before revealing it and decide exactly when it's revealed.

12. How are conflicts and confidentiality handled?

The system helps identify conflicts for the Grantmaker. In addition, the Grantmaker can enter conflicts and over-ride system identified conflicts and the reviewers can mark conflicts for themselves. If an application is marked as a conflict for a reviewer, the reviewer will only see the program name, applicant name, institution, and project title for the application. They will not be able to see any of the application details, critiques, or scores.

The system allows the Grantmaker to provide a Confidentialty and Conflict of Interest statement that the reviewers must read and accept before they can access the committee. If the reviewer does not accept the statement, they cannot proceed to the committee, review applications, or submit critiques. The Grantmaker has the option to make the reviewers accept the statement only the first time they log-in or every time. In addition, the Grantmaker can re-set the confidentiality acceptance at any point to make all the reviewers accept the next time they log-in, for example immediately before a review meeting.

13. How is proposalCENTRAL protected from failure of its servers or a regional disaster?

Wherever possible, Altum builds redundancy into its software and service architecture to ensure high availability. Altum's objective is a minimum of 99.9% availability, excluding normal scheduled maintenance or downtime caused by circumstances beyond Altum's reasonable control. To try to achieve this level of availability, Altum has implemented the following high availability processes:

A. **24x7 Automated Monitoring.** To ensure early fault detection and prompt response, all major hardware, software and network components of the Altum service are continuously monitored by software to automatically detect failures. The automated software monitoring operates 24x7.

B. **Automated Alerts.** If the monitoring software detects outage, the Altum operations manager and technical support are automatically notified via pager or cell phone. This alerting service operates 24x7.

C. **Database Transaction Logs.** Database transaction logs are backed up every 15 minutes. These transaction logs are also synced with a database server off site. File data is replicated to an offsite storage server every 2 hours. In case of failure of either of these servers, these backups are made to a completely separate server co-located with the production servers so that the backup server can operate as a hot spare for either or both the production web server and production database server.

D. **Twin Configuration.** Two web servers with identical configurations run at the same time with services split by a separate load balancing appliance (which also has its own failover unit). Two database servers also run together in a production and standby pair. Changes to the database are instantly replicated to its partner through Microsoft SQL Server Mirroring. A third server with SQL services monitors the partnership and health of the failover pair.

E. **Back Ups.** Application software is stored on both active and inactive web servers with identical configurations. Application software is also backed up to tape which is stored off-site.

F. **Redundant Components.** Altum's servers are configured with redundant hardware to reduce the impact of failure in any single hardware component. This includes redundant disk drives in either a RAID-1 ("mirrored") or RAID-5 ("striped") configuration; multiple Network Interface Cards (NICs); and dual power supplies . In addition to individual components, every piece of the network has two of everything, from load balancing, to switching, to servers.

G. **Secured Hosting.** Altum's hosting facility (ISP) is in McLean, VA (Level3 Communications). Level3 offers a state-of-the-art secure data center with high capacity redundant, peer Internet access to prevent problems with any individual network carrier(s) causing access related downtime. Level3 provides complete power protection with a battery backup system with emergency diesel generator power. Altum has 24×7 emergency access to its servers.

H. **Spares And Hot Swap Capability.** Altum has spare components (e.g., disk drives, memory, power supplies, NICs) available for immediate replacement in the event of a failure. Altum's servers are configured for "hot swap," enabling faulty parts, like disk drives, NICs or power supplies, to be replaced without shutting down the server. Altum also keeps 24x7x4 support on its hardware, so that if parts are needed, they are available from Altum's vendor in rapid response.

Disaster Recovery Plan. In the event of total loss of the current data center, Altum's recovery plan will utilize servers from its main business office and off-site backups which are physically separated from the production servers at the Level 3 data center. The offsite backups are encrypted and stored on the Amazon S3 cloud at its U.S. West Coast data center. The business office spare servers are configured with the current proposalCENTRAL code-base and the off-site backup of the production data and files so that they can replace the production servers. With this recovery plan, Altum expects to have the proposalCENTRAL service back in operation within 24 hours.