Security White Paper

When Member Campuses (or potential Members) ask "how secure is your application" or one of its variations, they are not really asking a specific question. While everyone is obviously concerned about security, what aspect of security are they really worried about? In general, what they are concerned about is "how can you ensure that our data will not get compromised"?

We have implemented various security measures at three different levels:

1. **Application Level:** This level is concerned with how we store our data, what data we collect, and what coding standards we have implemented to ensure our client's data is safe.

2. **Network Level:** This level is concerned with making sure data is not compromised as it goes "across the wire," securing the network via firewalls and monitoring, and ensuring we are running our software on the most secure platforms available with the latest patches and updates.

3. **Physical Level:** This level is concerned with physical access to the servers. While most people think of hackers of operating at the network level, theft and unauthorized access to servers by employees and other people within an organization is an actually a greater vulnerability than network "hackers".

Application Security

At the application level, we have implemented several security measures and coding standards to make sure the "front door" to our data is secure.

- **Coded to guard against common hacking techniques:** While we can't reveal what methods we have employed to guard against these methods (as revealing those methods would itself be a security leak), we have coded all our applications against common hacking techniques such as SQL injection attacks and cross-site scripting.

- **Password management:** One of the easiest ways to hack a site is to access it with a valid username and password. All of our passwords are encrypted using a one-way hash, which means password recovery is impossible, as it is not possible to decrypt the stored password. To reduce the possibility that passwords will be guessed, we have also employed rules to ensure that the "strength" of all passwords meet a minimum standard.

- **Latest, most secure platforms:** Our applications are built on the latest, most secure platforms in the industry. Our servers and applications are always patched with the latest security updates and releases when they are released by our server vendor.

Network Security

To protect our system at the network level, we have implemented the following measures:

- **Dual firewalls:** All our servers are behind two firewalls—one physical and one software, and employ strict recordkeeping of all firewall rules & logs; we have the ability to examine any and all additions/deletions to rules. With a concurrent versioning system we also have the ability to adjust to a previous setting if need be.

- **SSL Encryption:** All sensitive information is encrypted between the Internet and our servers with SSL.

- **24/7 Monitoring:** Our Network Operation Center (NOC) Operators have an understanding of what is usual versus unusual behavior for a server, monitored service (http, CPU loads, disk space thresholds, etc.), or a specific application being run. Some additional aspects of our monitoring software allow us to delve a bit deeper than a standard piece of software. With the ability and understanding of bandwidth monitoring; we can provide specific details as to what TCP/UDP protocol is using the most or least. Historical views enable staff members to relay all kinds of information including, but not limited to: time of day, week, month, and year. More importantly, in regards to security; if we see an unusual spike in traffic that is unwarranted we are able to react proactively & let our clients know.

- **Web-Enabled monitoring Software:** We have a web enabled application that allows us to view the status and information of our systems from anywhere on the internet. This gives us an intelligent view into a client's systems, ranging from detailed problem and metric display to long-term trending views, to overall calculated system health status.

Physical Security

To protect our systems at the physical level, our servers are housed within a Class A Data Center, compliant with TIA standards. Our network operations center has the following measures:

» **Always Staffed:** The most important aspect of physical security is the fact that our NOC is a true 24/7/365 data center. We always have a NOC Operations Specialist always present to monitor our security and infrastructure.

» **Access points (3 tiered):**

- 4-digit number code authentication to gain entrance to building lobby that is off-limits to public.
- RFID scanned logging of assigned cards with unique 4-digit code authentication for entrance to 3rd floor facility.
- An additional card scan required to gain entrance to through secured Data Center doors. Only approved staff members have permission or the ability to enter.

» **Camera Surveillance:** 24-hour camera surveillance with video archiving to ensure authorized personnel is identified upon entrance to building & data center floor. Picture ID badges to confirm identification is also required.

Security Audits and Disaster Recovery

Using proprietary monitoring, our engineers can (in real-time) realize any system abnormalities, traffic differentials (bandwidth spikes), CPU performance, & intrusion detection are just a few examples. No less than 5 members of our IT staff are notified immediately via SMS of any alert based on specified notification process. All alerts, warnings, & other incidents are documented within ticketing system and can be weighed or compared to past behaviors (historical data warehousing) with little effort.

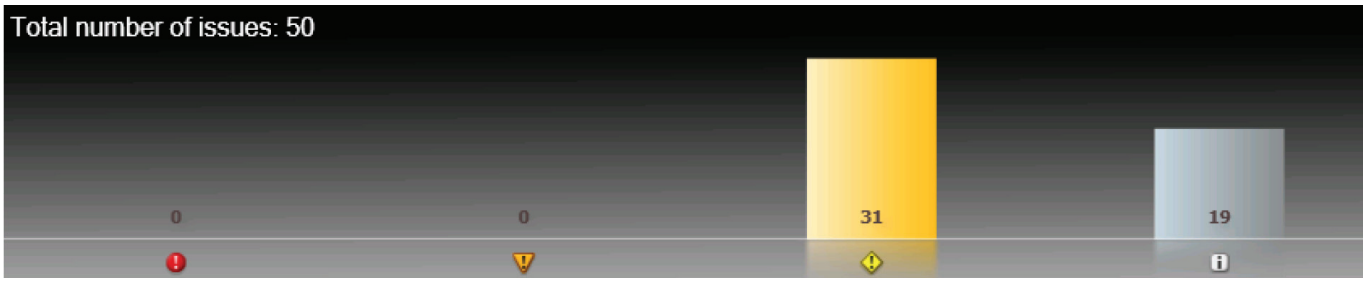
Network security audits are performed no less than bi-annually. All firewall (linux – iptables) rules are under versioning control to a central SVN server, with only two employees having the capability to make any changes (separation of duties). The firm responsible for regularly performing penetration/vulnerability assessments also provides these services for various government agencies.

Our hosting facility adheres to NIST 800-53 Rev. 3, which addresses security controls for Federal Information system in accordance with the security requirements in Federal Information Processing Standards (FIPS) 200. The security category that Shatter I.T's information system complies with is the moderate category. The entire specification can be obtained at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf.

A copy of our hosting facilities Compliance Overview document is available upon demand.

In addition to our in-house and 3rd party security audits, we are at times required to under-go application security inspections by our clients. These generally consist of using tools to crawl and scan our URL's. For example, we recently completed an extensive review with the University of Missouri-Columbia's Information Security and Account Management team. Their team used IBM Rational AppScan to do a deep inspection of our applications.

This scan looked for application vulnerabilities including, but not limited to SQL Injection attacks, ability to gather sensitive information such as usernames and password, or gain access to the underlying servers. This scan found no high or medium issues and the remaining issues have either been corrected, were false-positives, or informational:



Data Backup and Recovery

Our database backup strategy uses a combination of transaction log replication and block-level synchronization in conjunction with the SQL Server VSS Writer to help ensure your ability to recover SQL Server databases. After the initial baseline copy of data, two parallel processes enable continuous data protection with integrity:

1. Transaction logs are continuously synchronized to the our backup server, as often as every 15 minutes.

2. An "express full" uses the SQL Server VSS Writer to identify which blocks have changed in the entire production database, and sends just the updated blocks or fragments. This provides a complete and consistent image of the data files on the backup server.

Fully encrypted backups are rotated off-site weekly.

Disaster Recovery

While the details of our Business Continuity Plan is confidential , in the event of a catastrophic failure at our main data center, our application can be brought back online in either our datacenter in Toronto, or our home office in Buffalo in less than 4 hours. If this plan goes into action, all of our clients would be notified immediately.

In addition, Campus Labs is in the process of complying with the NFPA 1600 (2010 edition) standard for National Preparedness.

Support for Campus Integration (CollegiateLink Only)

CollegiateLink provides several points of integration with your campus systems. These integration points include:

1. Integration with Authentication Systems for Single Sign-On Capabilities
2. Data Import capabilities from your SIS system for use within CollegiateLink
3. Data Export capabilities to export data from CollegiateLink into a system of your choice.

Authentication Systems and Campus Portals

CollegiateLink may be configured to use your campus-wide authentication system to preserve your "single campus user account" methodology.

- All users log in with their current campus username and password
- User profile data is automatically populated for the user
- May be integrated into your campus portal for single-sign on

All authentication systems and portals are supported, including LDAP / Active Directory, CAS, Shibboleth, SCT Luminis, and custom configurations.

If the system is not configured to use a campus authentication system, users will be asked to create their own usernames and passwords.

Campus Authentication Integration Workflow Examples:

Example authentication process utilizing pass-through / token-based authentication system:

1. User clicks Login link on the CollegiateLink system website, which redirects the user to the campus authentication system's login page
2. User logs in with campus credentials and is redirected via SSL to the CollegiateLink site with a unique authentication token passed as part of the request (url parameter, cookie, etc)

3. CollegiateLink verifies the authentication token with the campus authentication system via a web service request, or based on an encrypted token showing that the request was made by a trusted provider during the last few seconds.

4. The CollegiateLink application presents the unique user identifier provided through authentication to any other campus systems to retrieve user profile information (web service, LDAP bind, etc).

5. User is logged into CollegiateLink. If this is the first time a user has logged in, a dialog is displayed presenting the user with the account registration form and privacy / usage policies drafted by the institution. User information may be populated based on step 4 above.

Example authentication process utilizing LDAPS or Active Directory over LDAPS:

1. User logs in through the CollegiateLink Web Application: Username and Password is transmitted from the web user to the CollegiateLink server via (HTTPS / SSL).

2. CollegiateLink connects to campus LDAP (using LDAPS encryption if available) using a read-only service account, and searches for a user DN associated with the given Username. CollegiateLink also gathers any necessary attributes for the user profile (including first name, last name, campus email, student ID, etc).

3. CollegiateLink performs a second LDAP bind using the DN result from above and the Password provided by the user. If successful, the user is authenticated. The Password is never persisted to the CollegiateLink database.

4. CollegiateLink logs user in. If this is the first time a user has logged in, a dialog presenting the user with the account registration form and privacy / usage policies drafted by the institution is displayed. User information may be populated based on step 2 above or via a subsequent call to other systems.

Data Import Capabilities (From an External System to CollegiateLink)

CollegiateLink now supports data imports from campus financial systems.

» Load financial transactions from your institution's financial system into CollegiateLink to show student organization account balances

» Import approved financial transaction requests from CollegiateLink into other accounting systems to automate check runs and purchase orders.

Data imports are supported from all commonly used financial systems such as Quickbooks, Dynamics, SAGE, and ERP (Banner Finance, PeopleSoft) so long as a flat-file of transactions and accounts can be exported from the campus system.

Automatic user data imports from your Student Information System may be configured to occur each time a user logs in as part of the authentication integration.

» Verify eligibility of students to vote in elections based on student status or other affiliation with university

» Supports all Student Information Systems including Banner, Datatel, PeopleSoft, and Jenzabar

Data Export Capabilities (From CollegiateLink to an External System)

A REST-based Web Services API is available for campus technology teams to query the CollegiateLink system. Documentation and access keys are provided on request.

» Store data on student participation and organization membership in your central data warehouse.

» Add verified co-curricular transcript data to your institutions official transcript

» Build web pages within your campus website, portal, or intranet containing information from CollegiateLink.

In addition, CollegiateLink supports open standards regarding event data, including iCal and RSS. Feeds may be used to import events from CollegiateLink into other campus calendars and facility management systems

Final Rule on FERPA

The Department of Education has released its much anticipated changes to the Family Educational Rights and Privacy Act (FERPA) on and effective December 9, 2008. The updates primarily consist of clarifications of past ambiguities, bringing light to previously contentious issues such as the definition of personally identifiable information and whether or not third party contractors are eligible to receive private student information. There are of course still some areas of debate, but the Department of Education hopes the new clarifications will provide a more detailed map as educators and administrators navigate through both emergency decisions and day-to-day management.

The proceeding summary of changes is not exhaustive of the FERPA final rule, but rather reflects the revisions which will in some way affect the proceedings of campuses in contract with Campus Labs. See "Implications" at the end of each section for especially pertinent information. Extended documentation can be found in appendices at the end of the document and read directly from the FERPA Final Rule.

Third Party Data Release

The Department has ruled that education records and personally identifiable information may be released—without consent—to third party vendors, volunteers, and non-employees under the following proviso:

- Contractors, volunteers, and any non-employees that have access to student records or identifying information must be included in the institution's Annual Notification of FERPA as "school officials with legitimate educational interests."

- Third parties performing institutional services must be under "direct control" of the institution

Implications for Campus Labs users

The third party release ruling came as a relief to most campuses, particularly those who have found a need to outsource institutional tasks to third party vendors. The term "direct control," which has stirred some debate, essentially implies that an institution must have and maintain ownership of all data released. In other words, an institution may not release data to any organization that intends to release or use that data for reasons outside the needs and requests of the university. In addition, third party vendors are also held responsible for the data released to them and universities and colleges should not release data to vendors who have or had policies of releasing confidential data.

Campus Labs complies with the FERPA ruling, as a "school official with legitimate educational interests," and can and ought to be listed as such in an institution's Annual Notification of FERPA. Campus Labs remains a responsible advocate for each of its campuses and does not and will not practice the release of data to any extent. Data released to Campus Labs is the property of the institution and under the direct control of that institution.

For a summary of the information detailed in the final rule, see Appendix 1. To view the official final rule, follow this link: http://www2.ed.gov/legislation/FedRegister/finrule/2000-3/070600a.html

Directory Information

The Department of Education has ruled that student ID numbers can now be included in directory information, given that they are not the sole identifier needed to access student education records. If used in combination with other identifying factors, student ID can be used to validate the identity of an individual who is requesting personal records.

Other provisos to note:

- Social Security numbers may not be included as directory information.
- SSNs may not be used to confirm directory information.
- SSNs may not be released without consent unless their release is
- SSNs may be used within intra-institutional communication (FERPA does not restrict a university from including SSNs on transcripts or other confidential documents), but only if SSNs are not the sole ID needed to access student education records.
- Universities and colleges must honor any student's request to opt out of releasing directory information. For current students, such a decision could significantly limit their ability to participate in technological communications (e.g., log-in to university site).
- A university or college must also honor the request of any former student who wishes to withhold his or her directory information from being released. Parents of former students may also opt out for their student.

Implications for Campus Labs users:

In the past, FERPA has ruled that student IDs could not be used as directory information for fear that the ID alone would provide access to confidential student education records. The new ruling clearly overturns this. FERPAs reasoning behind the change is largely in part to increased security measures on most campuses, where more than one identifying item is necessary to gain access to education records. With the increased measures to protect student identity, FERPA felt it was overly restrictive to maintain this ruling.

As a call to action, it will be important for educational institutions to inform themselves on the measures used to gain access to student education records. If a student ID is the sole piece of information needed to access these records, student IDs may not be used as directory information, nor released publicly without student consent. However, Campus Labs qualifies as a "school official" under FERPAs terms and as such institutions may release data—both directory and confidential—to Campus Labs without fear of negligent practice.

Personally Identifiable Information

Under the previous policy, personally identifiable information was described as any information that was "easily traceable" to the student's identity. In replace of this phrase, FERPA now provides the following standards for defining personally identifiable information:

- Any indirect identifiers such as mother's maiden name, place of birth, ethnicity, date of birth, etc.
- Information or a combination of information that would give a reasonable person in the school community, without personal knowledge of the situation, the ability to identify the student or students with reasonable certainty
- Information requested by a person whom the educational agency or institution reasonably suspects to know the identity of the student to whom the education record corresponds
- In addition to the items listed above, a new term "biometric record" has been added, which is defined as "a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting."

**It should be noted that under FERPA only parents and eligible students reserve the right to request student education records.*

Implications for Campus Labs users:

Because Campus Labs complies with the third party release rules stipulated under FERPA, personally identifiable information may be released to Campus Labs. The items above predominately affect communications inside a university and the extent to which personally identifiable information can be released publicly.

The Department of Education has written a detailed description of their reasoning behind these changes in the FERPA final rule. For a summary of some of the key debates cited in the final rule, see Appendix 2. To view the official final rule, follow this link: http://www2.ed.gov/legislation/FedRegister/finrule/2000-3/070600a.html

Appendix 1

Based on the new title "school official," The Department of Education does not suggest that any contractor now hold status as an institutional employee, but rather that they must "act for" the institution—as an employee of the institution would--and not use that information to solicit products and/or services to students and parents. (FERPA gives the example of an insurance company that might directly sell insurance plans to students.) Furthermore, the institution must maintain that they have ownership and control of the released data. FERPA does not require institutions to sign contracts with third party vendors, to be in direct supervision of the functions of the contractor, or require that the third party have verified safeguards against the release of private data; however, FERPA does recommend that institutions sign contracts detailing their ownership and control of the data, possibly including penalties for unauthorized release of that data.

Finally, both the institutions and educational agencies are "responsible under FERPA for ensuring that they themselves do not have a policy or practice of releasing, permitting the release of, or providing access to personally identifiable information from education records, except in accordance with FERPA."

Appendix 2

Some commentators have questioned the removal of the "easily traceable" phrase and others wonder if "ordinary person" might be a better approximation than "reasonable person." In response, the Department of Education has stated that "easily traceable" seemed to suggest that only information that was easy to trace back to the student would be included and of course information that may be difficult to trace back ought to be included in the definition. The Department disagrees with the recommendation to change "reasonable person" to "ordinary person" as they maintain that "reasonable person is a legally recognized standard that represents a hypothetical, rational, prudent, average individual."