



Web Applications

WHITE PAPER

**CLC TECHNOLOGY**  
SECURITY WHITEPAPER

*This document, concerning CLC Technology web application security is a statement of policy. Though it is not intended or expected, should any discrepancy occur between this document and the actual security controls and policies found at individual CLC Technology web application sites, the security controls and policies at the web site takes prominence. This paper is being made available solely as a means to facilitate the public's access to these policies.*

CLC Technology  
4170 Douglas Blvd.  
Granite Bay, CA 95746  
(866) 262-5750

## CONTENTS

Forward.....	1
Preparation .....	1
Usage Policy .....	1
Risk Analysis .....	1
Security Team .....	1
Best Practices .....	1
Prevention.....	2
Software Architecture .....	2
Encryption .....	2
Credit Card Data .....	3
Physical Facility .....	4
Monitoring .....	4
Virus and Malware.....	4
Response.....	4
Security Violations.....	4
Restoration .....	5
Review .....	5
HIPAA compliance .....	5
HIPAA Privacy Policy and Practices.....	5
Registered Users .....	5
Exchanges of Personal Information .....	5
Personal Information We Collect from Registered Users.....	6
Personal Information We Collect From Others .....	6
How We Protect Personal Information.....	6
When We Exchange Personal Information .....	6
Individual Rights .....	6
HIPAA Privacy Notice .....	7
Other Information.....	7

## **FORWARD**

Divided into three areas: *Preparation*, *Prevention*, and *Response*, this whitepaper discusses security for the software web applications designed and engineered by CLC Technology. This paper is not a full disclosure of all security practices and policies. For HIPAA compliance there is a review of our HIPAA Privacy Policies and Practices and additional HIPAA compliance information can be found at our sites that require HIPAA Notices.

## **PREPARATION**

### ***Usage Policy***

Deployments of CLC Technology web applications designed for client sites with access requiring a password have some combination of User Agreements, Software Licenses and Privacy Statements that must be agreed to prior to initial access of the site. Client based sites are engineered with client limitations to restrict use of the site to its intended purpose and to enforce some policies in the User Agreement and/or Software License without compromising the privacy of the clients data.

### ***Risk Analysis***

Software web application design, engineering and testing include comprehensive risk analysis measures at each phase of development. The core web application has a stringent design policy for security upon which all engineering takes place. The design policy for security exclusively deals with risk analysis and enforces the methodology by which we reduce risk at the source through design. The core web application is wrapped in an extensive hardware and software security shield.

Data center risk analysis is performed by an internal CLC team of network and hardware engineers. Based upon conventional risk analysis metrics, and using risk assessment software tool sets, regular risk testing and review of the data center is performed.

### ***Security Team***

Working together to address a broad range of security issues the CLC security team is comprised of the senior engineering staff along with the senior network and data center administrators.

### ***Best Practices***

The adherence to Best Practice methodologies is critical to supporting the health of web application security. Software design, development, testing and maintenance supported by our best practice policies enforced by change



management software are the foundation of our software development best practices.

The process for hardware best practices enforced by the data center director includes procedural jobs such as approval for changes to fire wall configuration, user identification changes, external partner access, changes to ACL's, the SNMP configuration, and assurance that the current software revision levels of network equipment and server environments are in compliance with the security configuration requirements.

Best practices extend to the hiring of staff. As part of our hiring procedure, CLC requires background checks and drug testing for all potential staff members. All CLC Technology employees have signed strict confidentiality agreements as part of their initial employment. Network access security levels are determined by CLC HR and departing employees go through a security debriefing exit interview, return access cards and their network access is removed.

---

## **PREVENTION**

### ***Software Architecture***

CLC Technology web applications are engineered employing the security methodology of RBAC<sub>3</sub> (Role Based Access Control) and a CLC Technology engineered version of RBAC<sub>x</sub>. Using compartmentalized software architecture complementary to the published Sensitive Compartmentalized Information (SCI) standards for U.S. Government security, CLC Technology web applications are hardened against outside intrusion. The web application compartmentalized architecture makes spoofing or reengineering of the URL virtually impossible, always resulting in an intruder attempt being directed to the login module without any page redirection. The security layer of the software, RBAC<sub>x</sub> controlled, restricts the user to their security permissions only, with no ability to move across unauthorized boundaries.

### ***Encryption***

The CLC Technology method of encryption is the Advanced Encryption Standard (AES) using the 256 key algorithms. In June 2003, the US Government announced that AES may be used for classified information. This is the statement from CNSS (Committee for National Security Systems) a division of the NSA (National Security Agency):



"The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths."

After user name and password login to any CLC Technology web application, all user data transmissions over the Internet, to and from our servers, is encrypted up to 256-bit SSL encryption. Up to 256-bit SSL (Secure Sockets Layer) provides a high level of encryption security protection whenever credit cards or other financial or confidential transactions are passed over the Internet.

The user's password database on CLC Technology servers is encrypted. There is no un-encryption key to the password database. Users must reset their passwords and receive an email with a temporary password they can reset to their old or new password. CLC Technology staff has no way to view the encrypted passwords or to gain access to the CLC Technology web application's private work groups.

All key data fields that contain data from user input or registration are encrypted.

CLC Technology web application user created data is unencrypted when you see it on the screen. The user data is encrypted by up to 256-bit SSL when it leaves your computer and travels over the Internet. When the data reaches the CLC Technology servers the encryption changes from up to 256-bit SSL to 256-bit AES. When it leaves our servers the encryption changes to up to 256-bit SSL as it travels back over the Internet to your computer.

### ***Credit Card Data***

This whitepaper will not fully discuss CLC Technology's methodology for management or protection of our customer's credit card information, because this paper is available to the public. Limited additional information is available through your CLC account representative based upon non-disclosure agreement.

The public facing information we make available is:

- The display of the credit card numbers to CLC staff or the holder of the credit card is only available in the xxxx-xxxx-xxxx-1234 format showing the last four digits.
- We have extensive and sophisticated policy, procedure and encryption of customer credit card information using the Advanced Encryption Standard (AES) described above.

### ***Physical Facility***

Our data center is in a state-of-the-art high-security facility, surrounded by barbed wire and guarded by armed personnel. Support technicians are at the facility 24 hours a day. We own and operate our own computer servers which are housed in our locked cabinets. User data is backed up and archived for retrieval, and production data is redundantly mirrored on CLC servers.

CLC Technology offices are located inside the CLC Incorporated building constructed for us in 2003. This building has recorded video surveillance inside and outside and is card control access secured 24/7, with unlocked front door during business hours and full time lobby receptionist.

Access to our internal server rooms are restricted to IT staff with proper security. Internal networks are protected by firewalls and centrally managed anti-virus. All access points are secured by username and password which auto-lock when left unattended. Our internal telephone systems are fully redundant and emergency backup powered to handle beyond maximum projected call volume.

### ***Monitoring***

The hardware and software performance in the datacenter is monitored with software monitoring and alert technology with messaging to computers, pagers and cell phones in the event of software or hardware problems. CLC has different levels of authority given to members of the security team to make changes, and in what order the changes should be made. Intrusion detection testing is the responsibility of the CLC security team and is constantly monitored.

### ***Virus and Malware***

Scanning and surveillance for viruses and unwanted executable programs takes place at the firewall, server and web application levels. The RBAC security and compartmentalized engineering design of the CLC Technology web application has made it impossible for viruses and illegal executable programs to spread through our CLC Technology web application.

---

## **RESPONSE**

### ***Security Violations***

CLC has adopted a comprehensive monitoring policy for each area identified through our risk analysis. Attempts to violate software or hardware security rules are automatically captured and logged to reports which are reviewed and assessed by the security team. CLC constantly monitors our internal network, our extranet and web applications for security violation attempts.

### ***Restoration***

Restoration of normal operations is the security team's final goal. Based upon our response decision, we determine how we conduct, secure and if required make available normal backups. Each of our systems has security conditions that permit restoration from backups.

### ***Review***

Reviewing the security policy against Best Practices keeps the web applications and network up to date. During security reviews CLC conducts the reviews according to policy, posture and practice. When reviewing security for the web application and network, its posture is compared to the security posture to maintain security policy compliance.

---

## **HIPAA COMPLIANCE**

### ***HIPAA Privacy Policy and Practices***

In addition to the previously described security policies and practices this section briefly reviews how and why the CLC Technology web application exchanges personal information about and for our Registered Users, how we handle that information and how it is shared on CLC Technology sites that require HIPAA compliance. We respect the privacy of personal information and handle it securely. Our practices apply to current and former Registered Users.

### ***Registered Users***

Individuals must register into the CLC Technology web application in order to use the service. This registration process creates Registered Users. There are two classes of Registered Users affected by HIPAA, (1) health care professionals that serve their clients and (2) the clients of the health care professional that were invited to the CLC Technology web application workgroup created by their health care professional for the purpose of serving their client.

NOTE: The CLC Technology web application does not verify the academic degree, credentials or professional licenses of Registered Users. It is the responsibility of the client to verify that they are exchanging information through a CLC Technology web application site with someone they trust as a competent health care professional.

### ***Exchanges of Personal Information***

Within the CLC Technology web application only the health care professional or the client have access to the secure online workgroup. Personal information is



put into the workgroup by either the health care professional or the client. No one else has access to the workgroup without the consent of the health care professional.

#### *Personal Information We Collect from Registered Users*

Registered Users must provide certain information when they subscribe or are invited to a CLC Technology web application workgroup. Based upon site requirements some of this information may or may not be required.

#### *Personal Information We Collect From Others*

We only collect personal information from Registered Users. No one else can arbitrarily use the system without being a Registered User.

#### *How We Protect Personal Information*

We use strict safeguards to protect the personal information of our Registered Users. These safeguards include how we store personal information in the CLC Technology web application workgroups and on our servers and how the CLC Technology web application exchanges that information between the health care professional and their clients. All personal information that can be entered into a HIPAA compliant CLC Technology web application workgroup is digitally encrypted and is not humanly readable except by the health care professional or their client. For very rare database technical issues, only the President and the senior engineer at CLC Technology can view the unencrypted personal information within the web application database, and this must be done in the presence of each other under tight and well documented security procedures, and can be accomplished only with the permission of the President. CLC Technology has never had the technical need to un-encrypt the HIPAA database for this purpose. CLC Technology cannot view or un-encrypt the encrypted Register User passwords. All lost or forgotten passwords must be reset by the Registered User or by customer service.

#### *When We Exchange Personal Information*

The CLC Technology web application does not and cannot exchange personal information on its own. Only humans can enter personal information for exchange into the CLC Technology web application and that can only be done with the permission and actions of the health care professional and the client.

#### *Individual Rights*

Our Registered Users can access the personal information they enter into a HIPAA compliant CLC Technology web application workgroup as long as the health care professional has not closed and caused the deletion of the workgroup. Once the health care professional closes a CLC Technology web



application HIPAA complaint workgroup the information contained within the workgroup is immediately and permanently deleted from the database servers.

*HIPAA Privacy Notice*

CLC Technology is required by federal law (the Health Insurance Portability and Accountability Act of 1996) to provide our Registered Users with this HIPAA notice describing their privacy practices.

*Other Information*

This document remains under review and will be frequently updated. We may change our privacy policy and practices from time to time. Please view our most current Privacy Statement available at the CLC Technology web sites. Privacy statements may vary by site based upon HIPAA and or site requirements.

*This document, concerning CLC Technology web application security is a statement of policy. Though it is not intended or expected, should any discrepancy occur between this document and the actual security controls and policies found at individual CLC Technology web application sites, the security controls and policies at the web site takes prominence. This paper is being made available solely as a means to facilitate the public's access to these policies.*