



The Corporate Giving Standard Security Overview

1. General Security

The Adage Technologies development team is responsible for monitoring and managing the security of the application and the infrastructure. Physical hardware is housed in a secure data center managed by IDC Global (www.idcglobal.net).

2. Physical Security

Equipment is hosted in a data center managed by IDC Global. The data center is physically isolated from everyone but level three technicians. Public access is strictly forbidden. Access to the data center floors is restricted to those holding IDC Global military-grade passcards. Physically, no one except level three technicians have access. Virtually, via L2TP/IPSEC VPN connection, only allowed from our office IP (enforced by the Firewall) and only the CGS development team.

3. Network Security

The CGS application infrastructure is air gapped from the Adage operating environment. The appropriate firewalling technology is in place and SHA-1 hash is used for encrypting passwords in the database.

4. Host Security

The ASP and the hosts comprising the application infrastructure have been hardened against attack in the following ways: Behind a firewall, security patches applied, only running the necessary services.

5. Account Security

Accounts are created by authorized CECP personnel. As a recent change, users cannot login to the CGS system directly. The login request comes from CECP public website, providing users with single sign on experience on both CECP website and CGS application. The transaction between CECP public website and CGS application is secure and uses two way handshaking, making it difficult for "man in the middle" attack.

Users can be disabled by an Administrator. A disabled user exists in the system but is not able to log in. A new user with the same login can NOT be created (usernames are unique).

Although CGS system does not allow direct login, during initial user creation, Passwords are created for the logins. This is entirely for the purpose of helping the CGS development team with the user experience. Passwords are stored in an encrypted format using SHA-1

6. Web Security

The application uses ASP.NET written in C# and Javascript. The application back-end is C# on the Microsoft .NET runtime.

Steps have been taken to mitigate the following common types of attacks:

- a. Use of and tampering with hidden fields.

Minimal numbers of hidden fields are used in the application and generally store non-interesting data such as the URL through which the user came to this page.

- b. Cookie "poisoning"

Session cookies contain only encrypted data. All other cookies are non-security related and contain only things to help the application remember view states such as the size of windows, current site section and the like.

- c. URL parameter tampering

Security checks are done on all parameters that are passed through the URL to verify that the current user has access to the given object in the system that the parameter denotes.

- d. Variable checking within application code

The application should not be vulnerable to buffer overruns or underruns or other stack-smashing attacks unless the underlying .NET framework is vulnerable. Similarly the application is vulnerable to format attacks only if the platform is. We don't do any SQL insertion.

- e. Buffer overflows within application code

Risk minimized by running in a sandboxed environment on the .NET platform.

7. Cryptography

Although CECP provides single sign on experience between CECP public website and CGS application, when users are created, new passwords are generated. This is purely for the purpose of helping the CGS development team with isolating any issues with the user experience. SHA-1 hash is used for encrypting passwords in the database.