NCCD National Council on Crime & Delinquency

SafeMeasures

Securing Confidential Information

The security of confidential data is of paramount importance to the National Council on Crime and Delinquency (NCCD). To ensure that all confidential data remain secure, NCCD has implemented a multi-pronged approach to Internet security that covers:

- Server configuration and network infrastructure;
- Transmission and storage of extracted data;
- Application access and communication; and
- Personnel policies and procedures.

Server Configuration and Network Infrastructure

The SafeMeasures® security model represents an extensive investment in the hardware and software necessary to keep confidential data secure. SafeMeasures uses multiple servers to store, receive, and display data. This allows strict control over access to data.

All SafeMeasures data are stored in an Oracle 11g data warehouse. Oracle's data storage methods ensure that no data are accessible nor readable by anyone without a valid Oracle user account.

All SafeMeasures servers are housed in their own locked racks within a secured server room at an Internet Service Provider (ISP) that is recognized for its ability to support and protect confidential data. The servers are protected using such safeguards as 24-hour video surveillance, escorted access, glass break detectors, and biometric scanners.

The Oracle database servers that hold confidential data are kept on an isolated network, apart from the servers that handle SafeMeasures' Internet traffic. These data servers are not accessible from the Internet and are completely isolated from and invisible to unauthorized users. To ensure they stay this way, the entire network and server infrastructure is regularly tested for vulnerabilities.

All access to the database servers is strictly limited. The SafeMeasures application accesses the data stored within these servers using secured web services that are only accessible to the code executing within the SafeMeasures application. Users cannot access these web services directly—the services may only be executed using the SafeMeasures code.

Whenever possible, the non-data files used to support SafeMeasures (templates, configuration files, etc.) are stored in private areas on each web server. When this cannot be achieved, any sensitive information that must be stored on a web server is always encrypted. This includes all user and database passwords.

Transmission and Storage of Extracted Data

In order to function properly, SafeMeasures requires data extracted from an agency's host system. NCCD has established procedures and systems to receive and store these data securely.

Data are extracted nightly via an automated extract and transmission program. This program is generally created either by NCCD or by agency personnel, and it runs within the agency's network environment. All data extracts are then compressed and encrypted, using industry-standard 256-bit AES encryption, before being sent to NCCD.

Data are sent to NCCD using the Secure Shell (SSH) protocol. SSH is a widely used method for securely accessing and transferring data to remote computers. SSH transmissions are encrypted and secured in several ways, including digital certificate authentication at both ends of the connection and encrypted password exchange. SSH uses RSA public key cryptography for its encryption.

NCCD takes the following measures to secure the incoming file transfer server.

- Firewall rules allow only SSH, SFTP, SCP, or FTPS/TLS connections from the Internet.
- All access is audited by user account and originating IP address.
- Audit logs are monitored regularly for malicious behavior, and NCCD maintains an IP blacklist on the firewall for any suspicious addresses.
- User accounts on the server are "jailed" using chroot, which is an operation that prevents one user account from accessing data in any other user account.
- NCCD recommends using RSA or DSA private/public key authentication for improved security and ease of scripting the automated process.

Application Access and Communication

Access to the SafeMeasures web servers may be restricted to a limited set of known IP addresses. This process, also known as "white listing," ensures that NCCD's web servers are accessed only by previously identified computers. However, it also prevents people from accessing SafeMeasures outside of their office (e.g., while working in the field) on their smart phones or tablets.

When enabled, white listing, in consort with other methods, hides NCCD applications from potential hackers, search engines, and random browsers. Most commonly, all IP addresses from agency offices are allowed initially; additional addresses can then be added as needed. Once a user's IP address has been recognized, he/she must log into the SafeMeasures application with a valid user name and password combination.

Aside from IP filtering, the SafeMeasures application utilizes current best-practice, audit-certified security features. These include:

- Email-based user account confirmation and password reset procedures;
- Network-level isolation of databases and data servers from the servers handling Internet traffic;
- Physical separation of user account and agency data on distinct database clusters;
- SSL encryption (see below for more information about SSL) of all traffic between the user's browser and the SafeMeasures website;
- Regular server penetration tests and other security audits by Qualys, a leading provider of Internet security services;
- Password complexity rules that follow agency requirements;
- Password aging and cycling rules that follow agency requirements;
- Account lock-out after five invalid login attempts;
- User-, group-, and role-based controls on access to specific pages, reports, and report elements; and
- User-level limits on the scope of visible data (e.g., limits to a specific unit or office).

All communications between the client browser and the SafeMeasures web servers are encrypted using the SSL protocol, which is the same method used to encrypt credit card and other financial transactions on the Internet. SSL encryption ensures that all data are protected while en route between the server and the client.

Personnel Policies and Procedures

NCCD has a long history of handling confidential information, the security and privacy of which will always remain a top priority. NCCD has implemented a number of policies and protocols to protect confidential data:

- By requiring all staff and consultants to sign confidentiality agreements as a condition of employment;
- By restricting access to the NCCD offices by locking all outer doors at all times; and
- By limiting access to confidential data to only key analytical and programming staff.

Further Information

For more information, contact:

Matt Wade, Director of SafeMeasures
426 South Yellowstone Drive
Madison, WI 53719

(800) 306-6223
mwade@nccdglobal.org

About NCCD

NCCD, the country's oldest nonprofit criminal justice research organization, was founded in 1907. Today NCCD works with agencies and organizations across 79 jurisdictions in the United States and nine jurisdictions in Australia, Canada, Bermuda, and Taiwan to develop and implement evidence-based and data-driven practices in adult and juvenile justice settings, child welfare, adult protective services, and other social welfare arenas. Please visit our website at www.nccdglobal.org. For more information, call us at (800) 306-6223.