Corporate CJIS Security Policy

Introduction

The purpose of this document is to provide an overview of CentralSquare Technologies, LLC's CJIS Security Plan, hereinafter "CentralSquare", to be utilized by CentralSquare personnel and customers. This document as well as referenced CentralSquare policies and procedures provide the groundwork to ensure compliance with the Federal CJIS Security Policy and state/local agencies that have implemented additional CJIS security requirements.

CentralSquare is a business partner serving law enforcement and other public safety organizations. As such, CentralSquare securely interacts with customer data and systems as described in this Security Plan. CentralSquare's Purchase Agreements with its customers, including law enforcement agencies, requires CentralSquare and its employees to maintain the confidentiality of customer data. Such data includes, but is not limited to, Criminal Justice Information (CJI), National Crime Information Center (NCIC) data, state specific CJI, and Health Insurance Portability and Accountability Act of 1996 (HIPAA).

One of the key standards used by CentralSquare in developing this Security Plan is the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division's Criminal Justice Information Services (CJIS) Security Policy. CentralSquare's CJIS Security Plan is periodically updated to ensure compliance with the latest active version of the Federal CJIS Security Policy.

Scope

The intent of this Security Plan is for CentralSquare to maintain a security program consistent with federal and state laws, regulations, and standards as well as the policies and standards formally adopted by our customer agencies.

The Security Plan identifies the standards with respect to the implementation and administration of appropriate internal controls so that the security and integrity of the customer agency's data, including criminal justice data and the FBI's information resources, are not compromised by CentralSquare personnel. This Security Plan describes the implementation of the security requirements outlined in the CJIS Security Policy, including:

- The process CentralSquare personnel follow to achieve CentralSquare Security Authorization;
- CentralSquare's process for documenting how its products comply with the Federal CJIS Security Policy;
- The process for maintaining site security through CentralSquare's secure facilities and infrastructure, and;
- The process for maintaining Customer system and data security through CentralSquare's security policies and procedures.

CentralSquare's security policies and procedures are available upon request by CentralSquare customers.

Security Authorized Personnel Standards and Training

CentralSquare personnel that must obtain Security Authorization include personnel involved in the implementation, configuration, support and upgrading of customer systems. This also includes those involved in the secure management of CJIS data, infrastructure and connectivity. This includes, but is not limited to, much of CentralSquare's Project Operations, Customer Service, Research & Design, Information Systems and Product Management teams. Select members of CentralSquare's Sales and Administrative teams may also be required to obtain Security Authorization.

CentralSquare Security Authorized personnel must complete the following:

- Pre-employment background check
  - This background check is performed by a commercial firm and includes records for all states. The check goes back to the beginning of time for the applicant. Candidates with felony convictions or disqualifying misdemeanor convictions are precluded from being employed in the Public Safety & Justice Division of CentralSquare. Candidates with outstanding warrants or pending criminal charges without a disposition are also precluded from being employed in the Public Safety & Justice Division of CentralSquare (pending disposition of the charges).

- Personnel Training
  - Security Authorized CentralSquare employees must successfully complete –
    - CJIS Online Security and Awareness training and testing. Certifications must remain current to maintain Security Authorization and must be renewed every two (2) years;
    - Various state and local agency mandated training and testing;
    - Internal CentralSquare required training and testing.

- Fingerprints
  - All Security Authorized personnel are required to be fingerprinted and have their prints submitted to one or more law enforcement agencies for a background check. In some cases, there is a state-wide specific process for fingerprint submission.

- CJIS Security Addendum
  - Security Authorized personnel are required to sign the CJIS Security Addendum Certification; copies are available upon request.

- Connectivity and Privacy Agreements
  - License and Support agreements include provisions for maintaining confidentiality of customer data. Customers may request additional documents for VPN and SecureLink/Bomgar access.

- Security Access Termination
  - Security access may be terminated for numerous reasons, including, but not limited to:
    - Termination of employment;
    - Transfer to a non-secure position;
    - Security authorized requirements expire or are no longer met.
  - CentralSquare has a defined procedure to manage the timely disabling of the individual's security access to facility, network, servers and data. CentralSquare will also notify customers of security changes, if required.
  - CentralSquare periodically publishes a list of Security Authorized personnel to customers.

- Site Security
  - CentralSquare facilities maintain on-site protection features, including:
    - Card key authentication required for building access;
    - Alarm system;
    - Secure server facilities with limited access;
    - Security cameras monitoring interior of facilities;
    - Policies and procedures for managing guest access.

- Secure Network Infrastructure
  - CentralSquare's network infrastructure includes appropriate firewalls, routers, intrusion monitoring, cloud storage and protection technology that meets~~,~~ or exceeds~~,~~ federal CJIS requirements. Documentation to support compliance is available upon request.

- CentralSquare Product Compliance
  - CentralSquare's Public Safety & Justice products meet~~,~~ or exceed~~,~~ federal CJIS requirements. Documentation to support compliance is available upon request.

- System Security (upon installation)
  - After CentralSquare's software products are installed and implemented at a customer site, the customer assumes responsibility for ensuring that they operate within the guidelines of their policies, procedures and CJIS security requirements. The customer's responsibility includes support and maintenance of their technical infrastructure, including updates for operating systems, database management software and updates to networks, routers and firewalls. The customer also manages personnel access along with password and Advanced Authentication.

- Data Management and Security
  - CentralSquare access customer data for the following purposes:
    - Implementation and configuration;
    - Data conversion;
    - Customer support;
    - System upgrades;
    - Any other legally or contractually permissible purpose.
  - In some situations, when performing these activities, customer data may be securely transmitted to CentralSquare. This is done with the customer's permission and data is stored in the secure area of CentralSquare's infrastructure that can only be accessed by CentralSquare Security Authorized personnel. Data is maintained for a limited time and a CJIS compliant process is followed for disposal of such data.

- CJIS Security Officer
  - CentralSquare had designated the Director of Compliance as the Security Officer responsible for developing this Plan. Currently, the Manager Data Privacy is responsible for developing, revising and/or maintaining same.

- Security Breaches
  - CentralSquare has an obligation to report a known breach of security using procedures outlined in the company's policies. Moreover, with respect to the UCJIS system, the Commissioner and Director of BCI will be notified if misuse of UCJIS information falls under reporting guidelines. Documentation, investigation, and notification procedures relating to a CJIS security breach meet or exceed federal CJIS requirements.

1) Version Control

Title	CJIS Security Plan			
Description				
Created By	Steve Weimer, Director – Compliance			
Date Created	4/1/2019			
Maintained By	CentralSquare Technologies Compliance Department			
Version Number	**Modified By**	**Modifications Made**	**Date Modified**	**Status**
1.0	Billie Jo Belcher, Manager Data Privacy	Amendment to Security Breach Section with respect to Utah BCI Audit April 2020.	April 19, 2020	