INSTITUTE FOR SOCIAL RESEARCH
UNIVERSITY OF MICHIGAN

CJARS Criminal Justice Administrative Records System

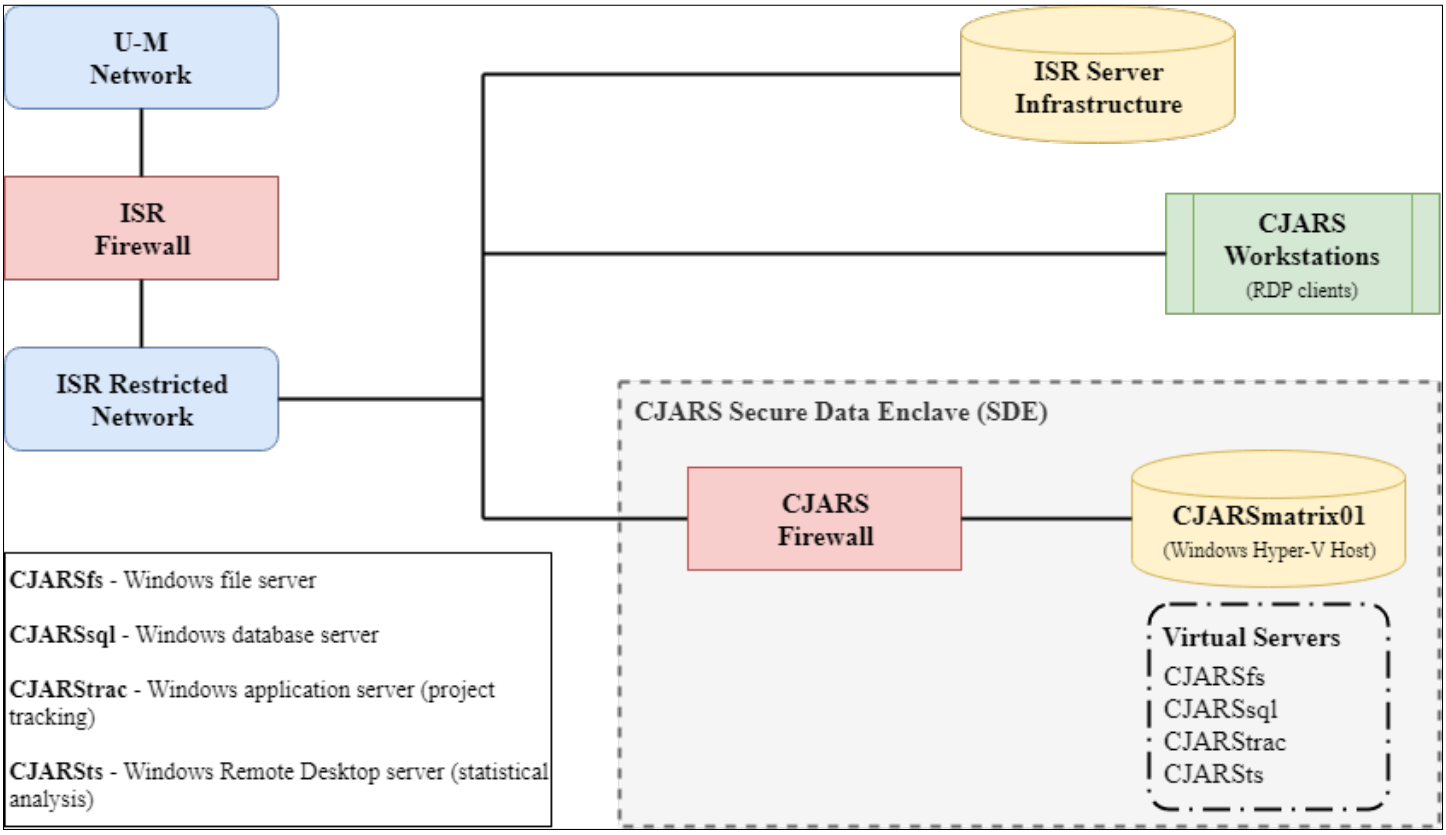
Data Security Summary

Introduction

The Criminal Justice Administrative Records System (CJARS) Data Security Summary provides an overview of procedures and guidelines for all staff, research partners, projects, and entities working with CJARS data. Although many records in CJARS are considered legally public, all are treated equally as Sensitive Personally Identifiable Information (PII) data. The CJARS secure computing environment was built to comply with all applicable FBI Criminal Justice Information Services (CJIS) data security requirements. This document outlines the technical specifications in place to ensure a secure computing environment.

System Overview

CJARS Secure Data Enclave (SDE) Network Diagram



Systems with externally-facing services are located behind a border firewall that is configured to only allow access to specific hosts and services. Systems that are only accessed internally are separated by another firewall with a limited set of exception rules that are reviewed and updated regularly. As a result, client workstations neither hold nor manipulate data locally to ensure sensitive PII data remain protected within the CJARS SDE boundary. This is enforced through both ingress and egress rules on the CJARS SDE firewall as well as RDP configuration settings that prohibit the redirection of local drives, printers, and clipboards.

426 Thompson Street
Ann Arbor, MI 48104-1248
https://cjars.org
(844) 864-8056

To protect and safeguard Sensitive PII, the CJARS research group performs their work on the Secure Data Enclave (SDE) via an encrypted Remote Desktop Protocol (RDP) connection to the CJARS "terminal server" (CJARSts) that requires a two-factor authentication. The SDE is a fully encrypted, dedicated physical server hosted on a private network by the University of Michigan (U-M) Institute for Social Research (ISR) and managed by the Survey Research Center's (SRC) Computing and Multimedia Technologies (CMT) department within ISR. In effect, the SDE is isolated from the greater ISR networks by a dedicated hardware firewall. This highly segmented network through the use of firewall devices provides additional layers of security for ISR systems. The table below details security and hardware specifications of the CJARS SDE server.

Physical Security	
Data Center	· Housed within 24x7x365 climate-controlled data center · Data center access protected by two-factor locked doors · Limited access to IT system administrators and authorized personnel with security badge
Surveillance	· 24x7x365 environmental condition monitoring · 24x7x365 motion-sensitive cameras that send pictures to designated personnel when triggered
Visitation	· Escorted at all times by ISR employee
Power	· 2x APC Smart-UPS 3000 to withstand brief outages
Server Security	
Identity & Access	· System authentication and authorization managed by Microsoft Active Directory (AD) · Sign Acceptable Use Policy and complete annual security awareness training to gain authorization via RDP connection · Multifactor authentication via Duo Security for RDP connection
Auditing & Accountability	· Network access monitored by automated intrusion detection system (IDS) · Data transfers into or out of SDE reviewed by the project PI or their direct delegate and logged using log correlation system · Audited system logins
Firewall	· Externally-facing services located behind border firewall to allow access to specific hosts and services · Internally-facing services separated by another firewall with a limited set of exception rules · Administrative access to network devices limited to encrypted protocols · Ingress and egress filtering to prevent unauthorized data exfiltration
Encryption	· Windows BitLocker full-disk encryption using 256-bit AES key
Backup	
Procedure	· Daily backups via enterprise-level disk-to-disk backup system · Full monthly backups written to encrypted tapes and stored in a locked, fire-resistant safe at a remote storage facility
Data Redundancy	· Daily hard copy backups encrypted and replicated between two physical buildings separated by two city blocks
Media Protection	· Transported in locked containers and attended by trained staff · Physically destroyed under staff supervision when no longer required
Hardware	
Processor (CPU)	· 3x Intel Xeon E5-2643 v3 Quad-Core CPU Processor 3.40 GHz
Number of Processors	· 12 (3x Quad-Core CPU)
Operating System	· Microsoft Windows NT 6.2 Server
System Type	· 64-bit Operating System, x64-based processor
System Memory (RAM)	· 256 GB
Hard Drive Capacity	· 2 TB
Hypervisor	· Windows Hyper-V Host Server (4 virtual servers for data management and analysis)
Project Management	· Trac Wiki System · Git Version Control

426 Thompson Street
Ann Arbor, MI 48104-1248
https://cjars.org
(844) 864-8056