Privacy & Security Training

Revised October 2023

Disclaimer

As of now, this presentation may be used for security awareness training for all user types. This can be used for initial training, but not continuous training. Agencies must have their own training tools that are used and updated annually per CJIS Policy AT-2.

Objectives

- Your role in privacy and security
- Laws and policies protecting information
- Penalties for violation

Privacy & Security

- User Security
  - Different roles
- Workplace Security
- Information Security

User Security

User Security

- Roles
- Background Checks
- Training
- Testing
- Logins
- Passwords

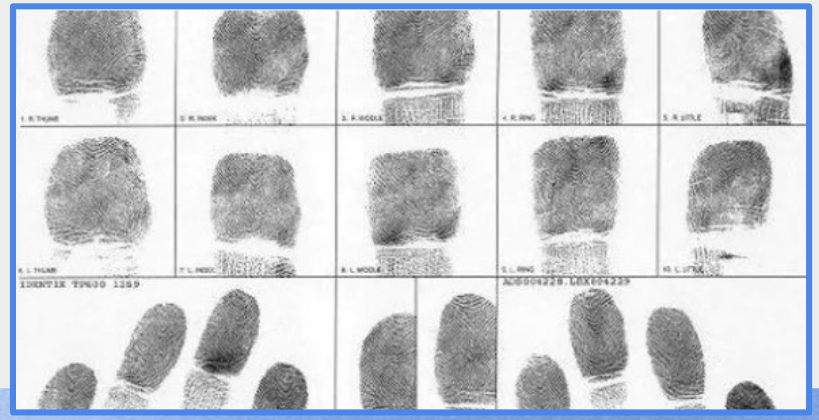
Roles

- CJIS Security policy now states that role based training be given to:
  - All individuals with unescorted access to a physically secure location (Non users)
  - General Users (Users and Non access users)
  - Privileged Users (Security administrators, system programmer, etc.)
  - Organizational Personnel with Security Responsibilities (LASO, Contractor, etc.)

CJIS Security Policy 5.2 AT-3

Background Checks

- Who needs it?
  - Everyone with access (direct or indirect) to UCJIS information or secured areas that house UCJIS information



Training

- New users &nonusers must be trained within six months of receiving their login
- Train at least once a year thereafter or:
  - After CJIS Security Policy Updates
  - Change in the information environment
  - When a security event happens
    - Training must be with the individuals involved

Testing

- New users must be tested within six months of receiving their login
- Tested every two years thereafter

Logins

- Login unique within your agency
- Login + ORI identifies you
- BCI tracks every transaction
- Log off UCJIS or lock workstation

Login Responsibility

- When something is accessed with your login, you will be held responsible for it

Passwords

- Do not use a dictionary word or name
  - admin, pass, pass2, passtwo, passpass
  - changeme
- Avoid personal information
  - Birthdays
  - Hobbies
  - Favorite sports team
  - Family members names
  - Friends
  - Pets

Passwords

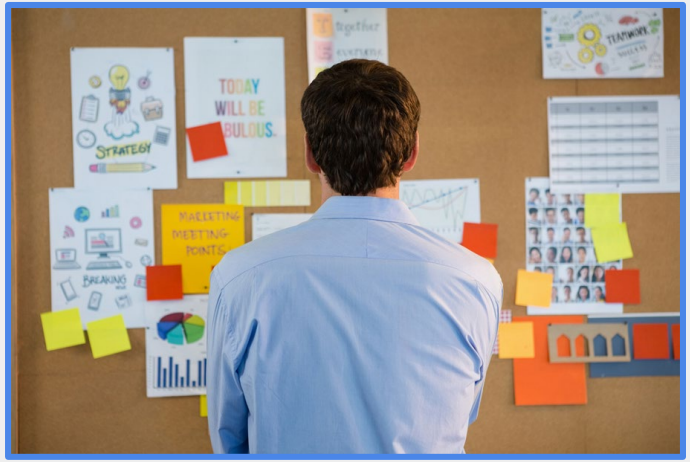
- Passwords must be eight characters including upper and lower case letters, numbers and the following special characters (!^*()_-=;:.’,[]{})
- Change your password every 90 days
  - Recommend every 45 days for system administrators

Passwords

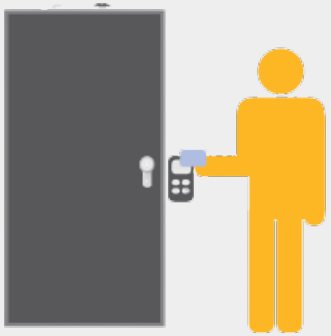
- Keep passwords confidential
- Never let anyone use your password
- If you think someone knows your password
  - Login to UCJIS and change it immediately
  - Contact your TAC or BCI

Passwords

- Where are some bad places to keep your password?



Workplace Security



Computer Sites

- Secure location
- Not visible by unauthorized persons
- Log off UCJIS when not in use
- Lock your screen

Visitors

- The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location
- Must be accompanied at all times
- Agency may choose to keep a visitor log

Workplace Security

- Public must not be able to view information
- Keep printouts in a secure area

Information Security

Information Security

- All UCJIS files are subject to
  - Federal, state, and local laws and policies

Information Security

- Firewalls, Spam, and Patch Updates
  - Network
  - Personal
    - Required for mobile devices
      - Manage program access to internet
      - Block unsolicited requests to access PC
      - Filter incoming traffic by IP, protocol or port
      - Maintain an IP traffic log

Information Security

- Wireless
  - WEP/WPA does not meet security requirements
  - WPA2 is a more secure connection and meets FIPS requirements

Information Security

- Laptops/Mobile Equipment
  - If used outside of a secured area, must have an Advanced (two-factor) Authentication (AA)
    - Something you know
    - Something you have/are
      - Includes biometrics

Information Security

- Mobile Devices
  - Advanced authentication (two-factor) or other compensation controls
  - Mobile Device Management (MDM) must be implemented
    - Password protection
    - Remote locking
    - Remote data deletion/wiping
    - Remote tracking

Information Security

- Personal Devices
  - Shall not be authorized unless the agency has established and documented the specific terms and conditions for usage
  - Shall be controlled in accordance with agency devices
    - Mobile Device Management

Information Security

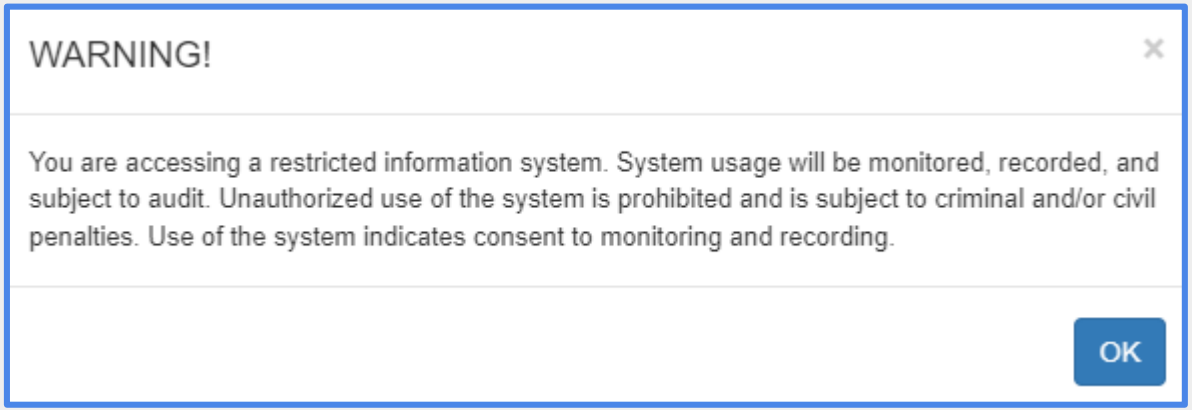
- UCA 53-10-108
  - Outlines restrictions on access, use, and contents of division records
  - (12)(a)It is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by the division or any information contained in a record created, maintained, or to which access is granted by the division for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

Information Security

- Data Backup and Storage
  - Centralized vs Decentralized

Information Security

- UCJIS Login Caveat



Accessing UCJIS

- UCJIS access is restricted to the following purposes:
  - Criminal Justice Employment
  - Criminal Justice Investigations

Criminal Justice Employment

- UCJIS Users
- UCJIS Non-Access Users
  - Individuals who do not access UCJIS directly, but receive UCJIS information such as judges, police chiefs, sheriffs, etc.
- UCJIS Non-Users
  - Unescorted individuals such as IT personnel, janitors, etc.

Criminal Justice Investigation

- Detection
- Apprehension
- Detention
- Pretrial release
- Post-trial release
- Prosecution
- Adjudication
- Correctional supervision
- Rehabilitation of offenders
- Criminal justice employment

Consequences of Misuse

- Violating security regulations can result in:
  - Civil lawsuits
  - Criminal prosecution
    - Class B Misdemeanor
  - Loss of access for User, Agency, or State

What is Dissemination?

- Giving UCJIS information to another person
  - Print, verbal, or electronic form

Dissemination

- If you disseminate information to an outside agency, you must document:
  - Who?
  - What?
  - When?
  - Why?
- Confirming if someone does or doesn't have a criminal history is dissemination

Information Destruction

- Printed Information
  - Burn
  - Cross-cut shred
- Electronic
  - Destroy all media with stored UCJIS information
    - Hard drives, CDs, Thumb drives, etc.
  - Thoroughly destroy or sanitize
  - Once released from your control, it must be unreadable

Social Engineering

- Techniques
  - Baiting
    - Asking a variety of questions to probe for information
  - Piggybacking or Tailgating
    - Following an authorized person through a secured entrance
  - Shoulder surfing
    - Viewing what is on a computer screen
    - Listening in on conversations

Social Engineering

- Techniques
  - Phishing
    - Emails asking for personal data or direct you to a website/phone number where they will ask for personal information
  - Spear phishing
    - Targeted form of phishing that targets a specific person of an organization in an attempt to access confidential data
    - Appears to come from a trusted source

Social Engineering

- Techniques
  - Pretexting
  - Impersonation
  - Quid pro quo
  - Thread-jacking
  - Social media Exploitation

Social Mining

- Social mining is an attempt to gather information about the organization that may be used to support future attacks

LASO

- Local Agency Security Officer
  - Identify users accessing UCJIS information
    - Protect against unauthorized use/access
    - Document connection to State system
    - Ensure personnel security procedures are followed
      - Includes security training

Incident Response

- To ensure protection of CJI, agencies shall:
  - Establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities;
  - Track, document, and report incidents to appropriate agency officials and/or authorities.

CJIS Security Policy 5.3

Threats and Vulnerabilities

- Threats
  - Natural disasters
  - Foreign and domestic
- Voice over Internet Protocol (VoIP)
  - Classical wiretap
  - IP phone netmask
  - Switch default password

Questions?