Privacy & Security

Objectives

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

Privacy & Security

- User Security
- Workplace Security
- Information Security

User Security

User Related Items:

- Background Checks
- Training
- Testing
- Logins
- Passwords

Background Checks

- Everyone with UCJIS access
  - Including those who see UCJIS info, but don’t a have login

Training

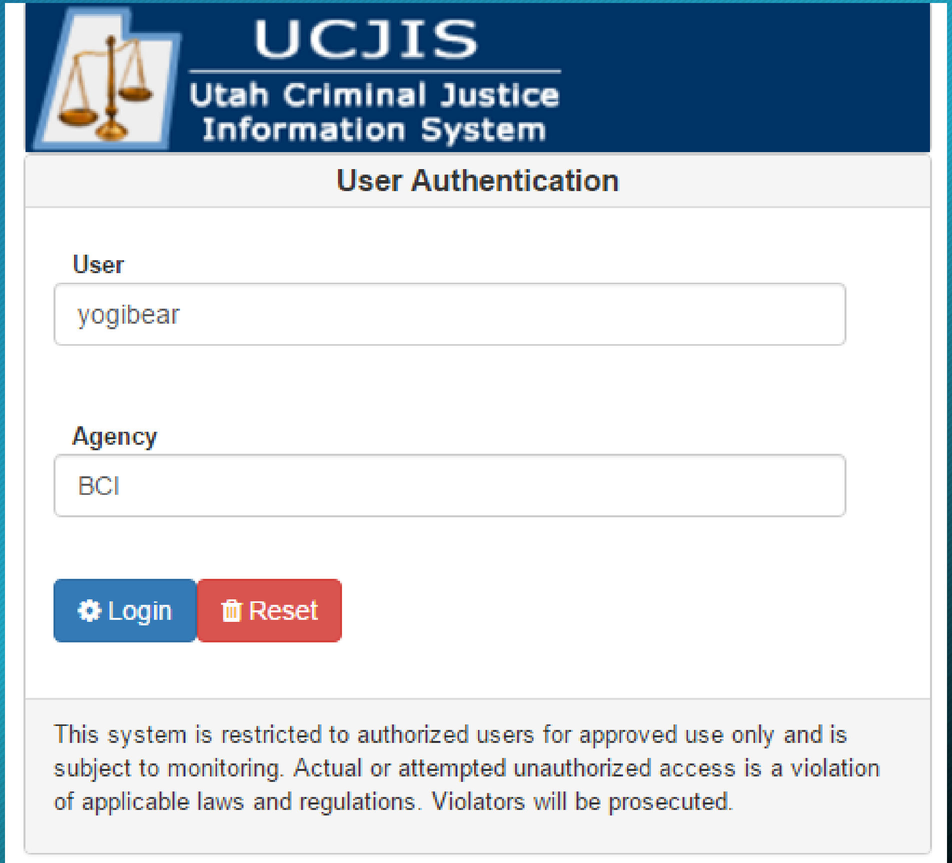
- New users trained within 6 months of getting login
- Train at least every 2 years thereafter
  - Any UCJIS updates

Testing

- Test new users within 6 months
- Test every 2 years thereafter

Logins

- Login unique within your agency
- **Login + ORI identifies you**
- BCI tracks every transaction made
- Log off UCJIS or lock work station



UCJIS
Utah Criminal Justice Information System

User Authentication

User
yogibear

Agency
BCI

This system is restricted to authorized users for approved use only and is subject to monitoring. Actual or attempted unauthorized access is a violation of applicable laws and regulations. Violators will be prosecuted.

Login Responsibility

Something accessed with your login?

You're held responsible for it

Security Awareness Training – **Passwords**

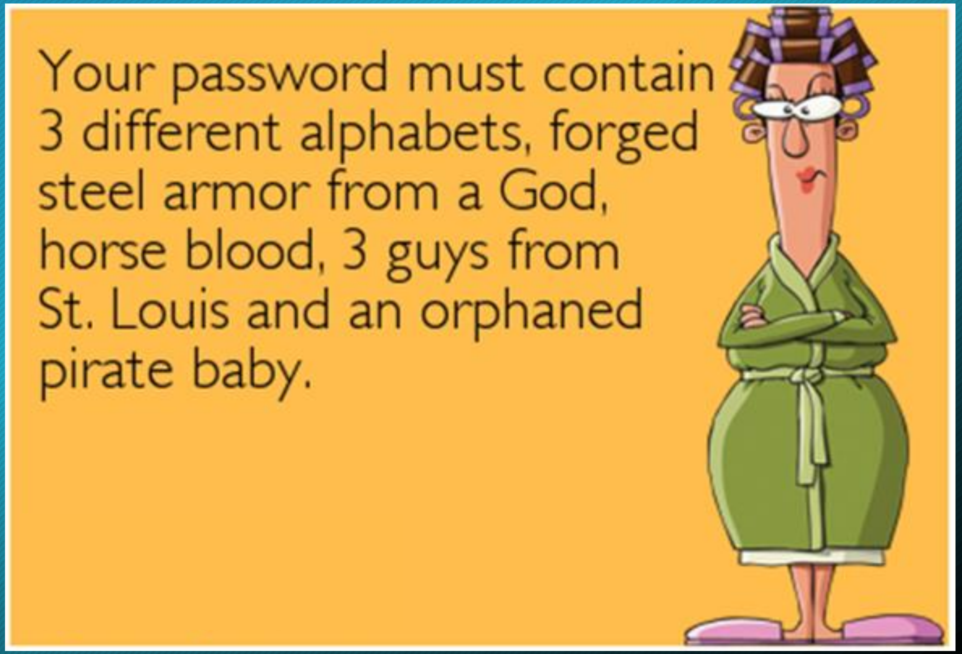
- Try not to use a dictionary word or name e.g. admin, pass, pass2, passtwo, passpass
- Avoid using personal information such as birthdays, hobbies, favorite sports teams, names of family, friends or pets

Security Awareness Training – Passwords

Passwords must be 8 characters including upper and lower case letters, numbers and the following special characters ! ^ * ( ) _ - = + ; : . ‘ , [ ] { }

Change passwords every 90 days

- Recommend every 45 days for system administrators



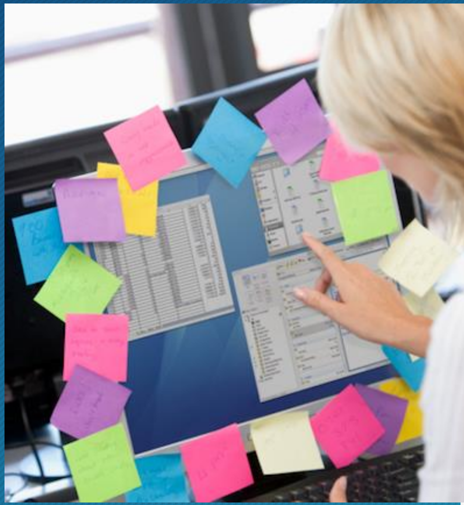
Your password must contain 3 different alphabets, forged steel armor from a God, horse blood, 3 guys from St. Louis and an orphaned pirate baby.

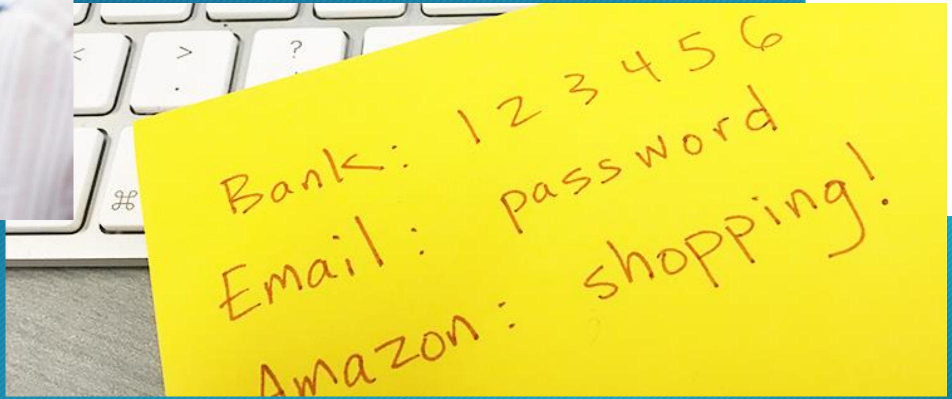
Passwords

- Keep passwords confidential
- NEVER let anyone use your password

Passwords

- Where are some bad places to keep them?





Passwords

Think someone knows your password?

- Go to UCJIS and change it immediately
- Contact your TAC/BCI

Workplace Security

Work Place Security

- Computer sites
  - Secure location
  - Not visible by unauthorized persons
  - Log off UCJIS when not in use
    - And lock your screen

Work Place Security

Visitors

- Must be accompanied at all times
  - Agency may choose to keep a visitor log

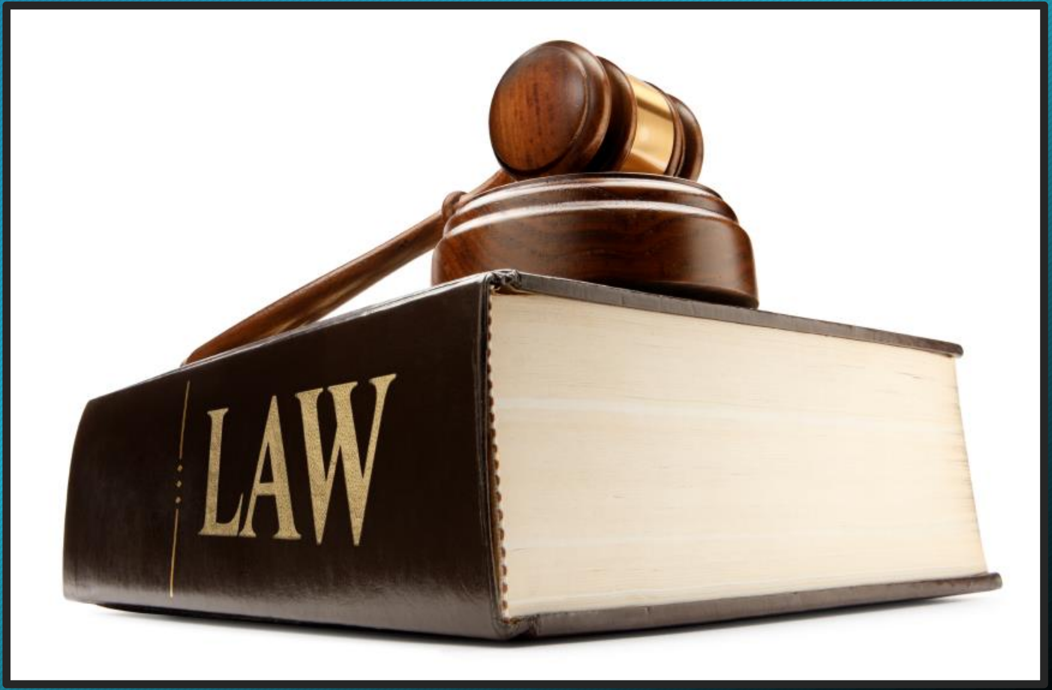
Work Place Security

- Public must not see Information
- Printouts kept in secure area

Information Security

Information Security

- All UCJIS files 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 secured area, must have Advanced (two-factor) Authentication (AA)
  - Something you know
  - Something you have/are
    - (includes biometrics)

Information Security

Mobile Devices

- Advanced authentication (two-factor) or other compensating 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

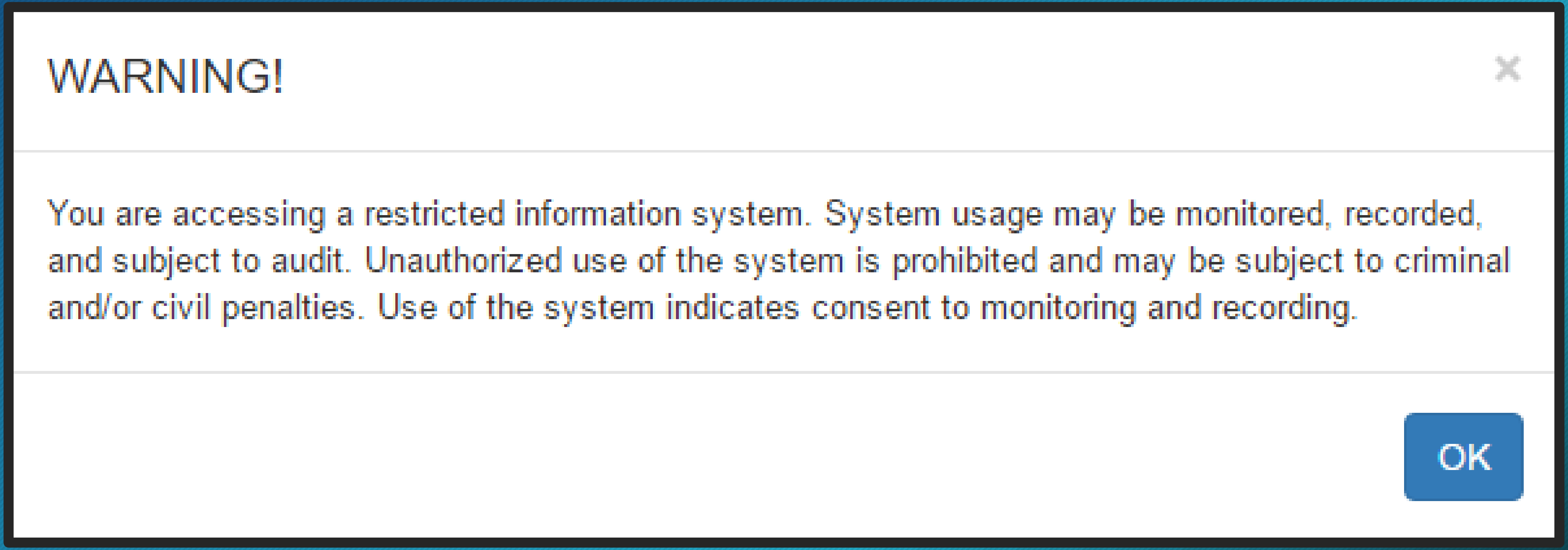
Data Backup and Storage

- Centralized vs Decentralized

Information Security - Utah

- Utah Code 53-10-108
  - Outlines restrictions on access, use, and contents of division records.
  - (12)(a) It is a **<u>class B misdemeanor</u>** 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 - Utah



WARNING!

You are accessing a restricted information system. System usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties. Use of the system indicates consent to monitoring and recording.

Reasons for Accessing UCJIS

UCJIS accessed for specific reasons

- Criminal Justice Investigations
- Criminal Justice Employment

Criminal Justice Employment

- UCJIS Users
- UCJIS Non-Access Users
- UCJIS Non-Users
  - Unescorted individuals such as IT personnel, janitors, etc.

Consequences of Misuse

- Violating security regulations can result in:
  - Civil lawsuits
  - Criminal prosecution
    - (Misdemeanor B)
  - Loss of access for User/Agency/State

Dissemination

- Giving UCJIS information to another person
- Whether in print, verbal, or electronic form
- If disseminating to outside agency, you must document who, what, when, and why
- Stating if someone does or does not have a criminal history is dissemination

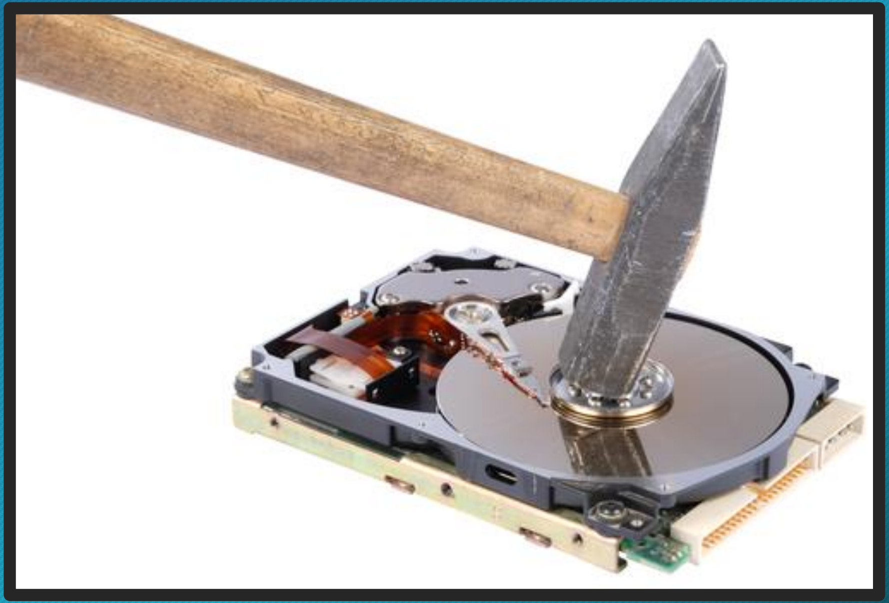
Information Destruction

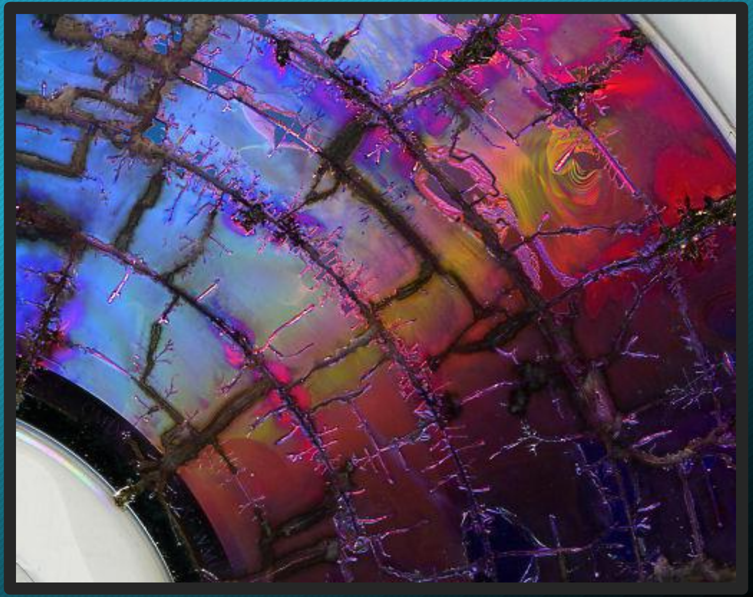
Paper

- Burn
- Shred (Cross shred)

Information Destruction

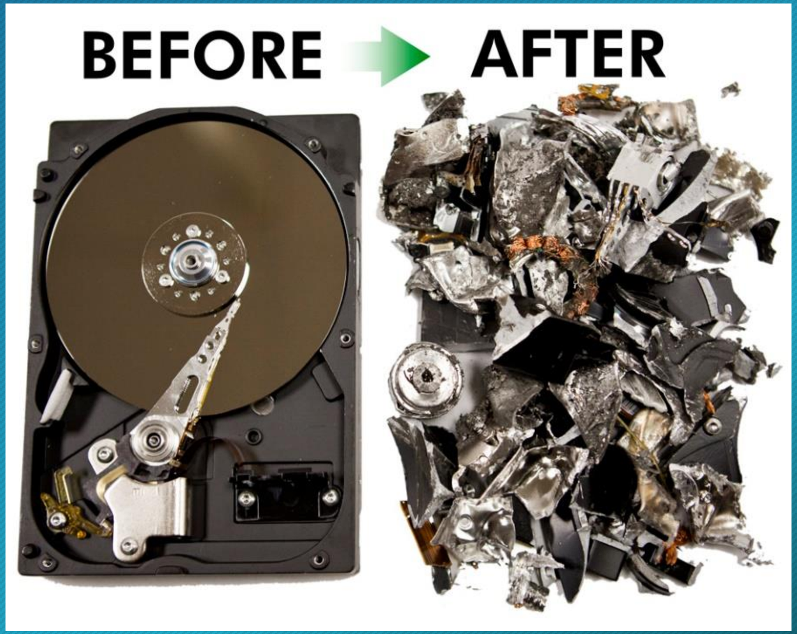
- Electronic media
- Destroy all media with stored criminal justice information
  - Hard drives
  - CDs
  - Thumb drives, etc.





Electronic Media

- Thoroughly destroyed or sanitized
- 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

Security Awareness Training- Phishing

- E-mails asking for personal data or direct you to a web site/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
    - Generally from a position of authority

LASO

- Local Agency Security Officer (LASO)

  -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

Incident Response

- "The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery."
- Agency shall promptly report incident information

Incident Response

- Action Plan

  -Priorities

  - Protect life
  - Protect information
  - Minimize disruption

  -Secure the system

Threats and Vulnerabilities

- Nature of Criminal Justice

  -Increased Scrutiny

  - Dependence on CJIS systems - enticing target for cyber attacks

Questions?