

## Part 2: Security Awareness Training



### CJIS Security Policy



- The essential premise is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit,
- Policies provide guidance for the creation, viewing, modification, transmission, dissemination, storage and destruction of CJI,
- Applies to every individual – contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity – with access to, or who operate in support of, criminal justice services and information.

## CJIS Security Policy - LASO

- The Patrol, as the CSA (CJIS Systems Agency) is responsible for ensuring each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO). (Ref: CJIS Security Policy 3.2.2)
  - All agencies are encouraged to download the electronic version at [www.fbi.gov](http://www.fbi.gov)
  - Appendix J of the CJIS Security Policy provides supplemental guidance for noncriminal justice agencies.

## LASO - School Districts

- Each agency having access to CJI must have someone designated as the LASO.
  - Although DESE is the holder of the ORI, we recommend that, in addition to DESE, each school district have a designated LASO as well.
  - Enable school districts to report incidents that occur at the district level directly to the MSHP/ISO.
  - Ensure compliance at the district level regarding section 3.2.9 of CJIS Security Policy.

## Each LASO shall:

- Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
- Identify and document how the equipment is connected to the state system.
- Ensure that personnel security screening procedures are being followed.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

## What is CJI?

- CJI is Criminal Justice Information- collected by FBI, MSHP and other criminal justice entities.
- Not limited to criminal history or information - also includes PII (Personally Identifiable Information)
  - PII is information which can be used to distinguish or trace an individual's identity.
- Available to criminal and noncriminal agencies authorized to receive information from CJIS systems.

## What is your responsibility?

- Information contained within and obtained from CJIS Systems is sensitive information.
- Improper access, use, and dissemination of CJIS data is serious.
- May result in administrative sanctions, including:
  - Termination of services
  - State/federal criminal penalties

## Dissemination

- Only use the information to perform your job duties.
- Do not disclose or share information with anyone that is not authorized to have access to the information.
- If releasing to another authorized agency, a log must be kept of the dissemination.
- Information needs to be protected from creation to destruction.
- Be aware of where information could go if released.

## The Reality

- Can we prevent every possible data loss or attack?
  - No
- Can we prevent every possible crime from occurring?
  - No
- Do we have a responsibility to the public to invest all **practical** resources toward protecting data?
  - Yes

“Security in IT is like locking your house or car – it doesn't stop the bad guys, but if it's good enough, they may move on to an easier target.” — Paul Herbka

## Implications of Noncompliance

### **Civil:**

Nearly Unlimited.

Elements of Negligence:

1. Duty of Care
2. Breach of Duty
3. Factual Causation
4. Damages

## Misuse

- Deputy Clerk at St Louis Circuit Court
- 48 counts of misuse of official information
- Access of criminal history, arrest records and Department of Revenue information
- For personal or private use
- Accessed/viewed information on herself and for friends, family and others.



## Security Incident

- An incident is the act of violating an explicit or implied security policy.
- These include, but are not limited to:
  - Attempts (failed or successful) to gain unauthorized access to a system or its data.
  - Unwanted disruption or denial of service.
  - The unauthorized use of a system for the processing or storage of data.
  - Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.

## Who should you report incidents to?

- Report security incidents to your LASO.
  - Your agency LASO will report the incident to the appropriate people.
- The MSHP Information Security Unit Email is:
  - [cjissecurity@mshp.dps.mo.gov](mailto:cjissecurity@mshp.dps.mo.gov)
  - Phone Number: (573) 522-3820
- Or, contact your Regional Auditor/Trainer for assistance.

## Security Incident Response Plan

- Should be part of your agency policy and procedure.
- If you are suspicious of something, report it through your agency's procedures.
- It is better to have multiple false alarms than miss one incident.
- The plan extends to a threat against any CJI – not just computer related – also includes physical media.

## Media Protection

- Electronic Media includes flash drives, hard drives, CD, DVDs.
- Physical Media includes documents, pictures, etc.
- All Media must be stored in secure areas.
- Access to Media should be granted to authorized personnel only.
- Ensure printed information is printed to the correct printer.

## Media Protection (cont'd)

- All CJI data located, transmitted or transported outside a secure location must be encrypted, according to FBI standards or carried in a locked container.
- Physical Media must also be protected in transit – it should be carried in locked container or folders where it is not visible to the public.

## Media Disposal

- Electronic Media must be physically destroyed or overwrite three times
- Physical Media must be shredded or incinerated.
- Put paper Media in shredding bins (marked for shredding.)
- Give electronic Media to your agency's IT personnel.



What's in YOUR trash can?

## Physical Security of CJI

- For handling of CJI, staff and equipment must be in a secure location – free from public access.
- The location could be a building, room or area.
- The area must be marked.
- List of authorized users must be maintained.
- Must have controls such as locks to verify individual before granting access.
- Computer or Information System Equipment area must also be in secure locations.

## Physical Security (cont'd)

- Computer monitors and printers must be secure in order to prevent unauthorized viewing.
- Visitor access must be controlled and logged if allowed in secure areas.
- Visitors must be escorted and monitored at all times.
- A visitor log is recommended.
- Recommend logging of any Information Systems related items, such as laptops, Ipads, handhelds, etc., entering and exiting the area.

## Threats to Systems

- A threat is an unintentional or deliberate event or circumstance which could have an adverse impact on an information system.
- Threats comes from internal or external sources.
  - Natural Threats
  - Unintentional Threats
  - Intentional Threats

## Threats (cont'd)

- Natural threats can endanger any facility or piece of equipment and include:
  - Fire, Flood
  - Lightning and Power Failures
- Unintentional Threats are actions that occur due to lack of knowledge or through carelessness and include:
  - Physical damage to equipment
  - Deleting information
  - Permitting unauthorized users access to information.

## Threats (cont'd)

- Intentional threats are those that are deliberately designed to harm or manipulate an information system.
- System software such as antivirus programs are designed to protect against these threats.
- Intentional threats include:
  - Social engineering, phishing,
  - Sabotage, Eavesdropping,
  - Unauthorized data access, intrusions
  - Denial of Service and Theft

## Malicious Code

- Includes viruses, malware, spyware and other code that is part of the code on a machine that does not fit into the standard configuration.
- Can be loaded intentionally or unintentionally.
- Could potentially disrupt the normal processing of a computer system.
- Be careful of websites or applications that ask to load software of your machine.
- Always have your IT install software.

## Email and Attachments

- Email is not secure unless you have a secure network.
  - Generally, do not send anything in an email that you don't want others to see.
- Do not send CJI in email unless you have proper technical controls in place.
- All email should be scanned for viruses and spam.
- Do not respond or open emails from unknown senders.

## Social Engineering

- Is the attempt to gather information by deception
- Scams and phishing attempts are the major categories.
- Could be by Email, telephone, face to face
  - Trying to gather information, such as a marketing call.
- If you are suspicious, report the incident.

## Laptops, Handhelds and Personal Devices

- Know your agency's policy on using these devices.
- Devices need to be secure and managed by your agency's IT staff.
- Need to be password protected/encrypted.
- If lost or stolen, report it as an incident.
- Be aware of screen location – avoid shoulder surfing – use screen savers.
- Always lock device before leaving it unattended.
- Personal and public devices are not allowed to access CJI system information.

## Advanced Authentication

- What is it?
  - An additional layer of verifying identity
  - Something you know: userid/password
  - Something you have: token/proximity card/bingo card
  - Something you are: biometric –fingerprint/ iris
- Must use 2 out of 3 categories to meet AA requirement.
- Must be used when accessing CJI outside of a secure location.

## Access Requests

- Should be a documented process.
- The main focus is separation of duties and least privileged access.
- A person who authorizes access should not have the ability to implement the request.
- The level of access should be enough to perform the job duties - do not give higher authority unless needed.
  - If your User ID is compromised, and you have least level of access, the less information is at risk.

## Use Policy

- This is a legal statement you agree to when you log-in to your computer or an application.
  - You should read it – it tells you what you can and cannot do!
  - Similar to the paper agreements you have signed for confidentiality.
  - This should be a part of sign-on for all information systems.

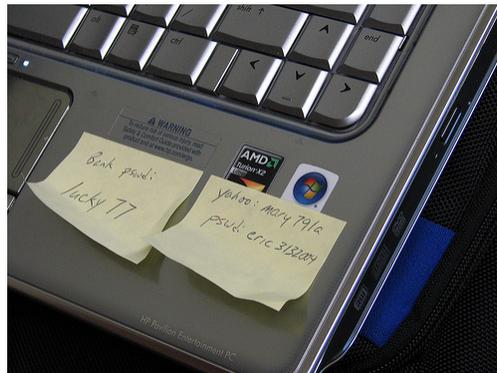
## Password Policy

- Minimum length of 8 characters
- Cannot be a dictionary word or proper name
- Cannot be User ID
- Will expire every 90 days
- Cannot be identical to previous 10 passwords
- Cannot be transmitted in the clear
- Cannot be displayed when entered

## Password Recommendation

- Do not share your password with anyone, not even your IT staff.
- Do not write down your password.
- Try not to increment numbers in the password
- Good passwords can be:
  - Phrases or run words together
  - Substitute special characters for common letters
    - \$omething2remember

## Do not write down or post your password



Not a good idea!

## Your Responsibility

- Make every reasonable effort to protect the information that you have access to.
- Protect the information systems equipment you work with.
- Report computer security incidents immediately. Containment is easier during the initial stages.
- Be aware of who is asking for information.

## Implications of Noncompliance

### **Misuse of official information - Section 576.050 RSMo**

2. A person commits this crime if he or she knowingly obtains or recklessly discloses information from the Missouri uniform law enforcement system (MULES) or the National Crime Information Center System (NCIC), or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job.

3. Misuse of official information is a class A misdemeanor

## Summary

- Protect from creation to destruction
- Be aware of information flow – where it can go, who is receiving and for what purpose.
  - Providing too much information may allow misuses of the information.
- Make every reasonable effort to protect the information.
- Protect the information systems equipment you work with.
- Report security incidents immediately --
  - Containment is easier during the initial stages.
- Be aware of who is asking for information.

## Report Security Incidents to:

State Information Security Officer  
(ISO) Mr. Patrick Woods

IT Security Specialist – Policy/Audit  
Ms. Hannah Vinson

(573) 526-6153

Email: [cjissecurity@mshp.dps.mo.gov](mailto:cjissecurity@mshp.dps.mo.gov)



## Contact Information

### Region 1- West/Northwest and Southwest

- Ms. Linda S. Lueckenhoff
- (573) 526-6153 extension 2630
- Email: [Linda.Lueckenhoff@mshp.dps.mo.gov](mailto:Linda.Lueckenhoff@mshp.dps.mo.gov)

### Region 2 – Central/North and South

- Ms. Valerie Hampton
- (573) 526-6153 extension 2655
- Email: [Valerie.Hampton@mshp.dps.mo.gov](mailto:Valerie.Hampton@mshp.dps.mo.gov)

### Region 3 – East and Southeast

- Ms. Pamela Aberle
- (573) 526-6153 extension 2625
- Email: [Pamela.Aberle@mshp.dps.mo.gov](mailto:Pamela.Aberle@mshp.dps.mo.gov)