Security Awareness Training

MSHP Information Security Unit

1. What is CJI?
   - CJI is criminal justice information
   - CJI is any information collected by FBI, MSHP and other criminal justice entities
   - It is available to anyone who is authorized to use CJIS systems – MULES, MoDEx, REJIS etc
   - CJI is not limited to criminal history or information available through MULES but can also include CAD, RMS, and MCD/MDT systems.
   - Includes PII (Personally Identifiable Information) and other derived information
   - This definition has changed from previous years – it is broader to include all information directly from state and federal systems but also data derived from those sources.

2. What is your responsibility?
   Information contained within and obtained from the CJIS Information Systems is sensitive information.
   Improper access, use, and dissemination of CJIS data is serious, and may result in the imposition of administrative sanctions including termination of services, as well as state/federal criminal penalties.

   YOUR RESPONSIBILITY IS TO PROTECT THE INFORMATION AND REPORT SECURITY INCIDENTS

3. What happens if you misuse CJI?
   Misuse of official information 576.050.
   - 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.
   - Misuse of official information is a class A misdemeanor

4. 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 i.e. the authorized individual/agency will have an agreement with your agency.
   - If releasing to another authorized agency that is not part of the agreement – 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

5. Why the big deal about protecting information?
   - In 2013 the average cost for the loss of a single record - $188
   - The average breach results in the loss of around 28,000 records
   - 28,000x$188.00=approximately $5.2 Million in damages for an average breach
   - Fines - $150,000 per incident
   - Indirect costs are even higher
   - Civil liabilities can be almost limitless
   - Loss of public confidence is the most damaging aspect for public safety

6. Who should you report security incidents to?
   Report your incidents to the TAC or LASO of your agency - they will report the incident to the appropriate people
   For Patrol employees, security incidents should be reported to the Patrol's Information Security Unit in the CJIS division at the contact information below:

   - MSHP Information Security Unit – email: cjissecurity@mshp.dps.mo.gov
     Phone: 573-522-3820

   CJIS Security Administrators
   - CSA - CJIS Systems Agency/ MSHP
   - CSO - CJIS Systems Officer/ Major Sarah Eberhard - MSHP
   - ISO - Information Security Officer/ Patrick Woods - MSHP
   - TAA -Terminal Agency Administrator/ Sheriff or Chief
   - TAC - Terminal Agency Coordinator/ Assigned at the MULES agency
   - LASO - Local Agency Security Officer/Assigned at agency with access to CJI

   Terminal Agency Coordinator (**TAC**) - The person in your agency responsible for the MULES computer system & operator access. They have the highest level of certification at your agency and must be a full-time employee. The TAC maintains MULES security for your agency's Computer Center

   Local Agency Security Officer (LASO)
   - Maintains list of users who have access to CJI
   - Identify how equipment is connected to MSHP
   - Ensures proper personnel screening procedures are being followed
     - Fingerprint check personnel that have unescorted access to secured locations
   - Ensure security measures are in place and working
   - Notify MSHP ISO of any security incidents at local agencies -
     MSHP Information Security Unit - email:cjissecurity@mshp.dps.mo.gov
     Phone: 573-522-3820

7. Incident Response Plan
   Definition of an incident - An incident is the act of violating an explicit or implied security policy.
   These include, but are not limited to:
   - attempts (either 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

8. Security Incident Response Plan
   - The Security Incident Response Plan should be part of your agencies policies and procedures.
   - If you are suspicious of something, report it through your agencies 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

9. Media Protection
   - The protection must include both physical and electronic media
   - 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
   - Make sure printed information is printed to the correct printer
   - 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

10. Media Disposal
    - All CJI data must be properly disposed of
    - Electronic media must be physically destroyed or overwrite three times
    - Physical media must be shredded or incinerated
    - Put paper media in shredding bins
    - Give electronic media to your agency's IT staff

11. Physical Security
    - In order to handle or process CJI, staff and equipment must be in a secure location
    - The location could be a building, room, area

- Area must be marked
- List of authorized users must be maintained
- Must have controls such as locks to verify individual before granting access
- Computer and Information system equipment areas must also be secure locations
- Monitors and printers must be secure in order to prevent unauthorized viewing of CJI
- Visitor access must be controlled and logged in secure locations
- Visitors must be escorted and monitored at all times
- It is recommended visitor log is maintained
- Information systems related items (laptops, IPads, handhelds, etc) entering and exiting the area are recommended to be controlled or noted on visitor logs

12. Vulnerabilities
    Vulnerabilities are points in systems that are susceptible to attack.

    Vulnerabilities may include:
    - Physical
    - Natural
    - Media
    - Human
    - Communication
    - Hardware and Software

13. Threats
    - A threat is an unintentional or deliberate event or circumstance which could have an adverse impact on an information system. Threats can come from internal or external sources.
    - One way to think about threats vs. vulnerabilities vs. risk:
        - A hole in a roof is a **vulnerability**
        - The rain is a **threat**
        - **Risk** is determined by the forecast or how likely it is to rain
    - Just like in the example above, risk determines how severe the treat or vulnerability is to your environment, I.T. or otherwise.

14. Natural Threats
    Natural threats can endanger any facility or piece of equipment. You may not be able to prevent a natural disaster, but damage can be minimized with proper planning. Natural threats include:
    - Fire
    - Flood
    - Lightning
    - Power Failures

15. Unintentional Threats

Unintentional threats are actions that occur due to lack of knowledge or through carelessness. These threats can be prevented through awareness and training.

Unintentional threats include:

- Physical damage to equipment
- Deleting information
- Permitting unauthorized users to access information

16. Intentional Threats

Intentional threats are those threats that are deliberately designed to harm or manipulate an information system, its software and/or data. Security software such as an antivirus program is designed to protect against intentional threats.

Intentional threats include:

- Social Engineering
- Phishing
- Sabotage
- Eavesdropping
- Unauthorized data access
- Intrusions
- Denial of Service
- Theft

17. Acceptable Use Policy

This is a legal statement you agree to when you login 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
- This should be a part of sign on for all information systems

18. Password Policy

- Your agency's password policy should be:
- 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
- Do not share with anyone (including your agency IT staff)
- Do not write down
- Try not to increment numbers in the password
- Make it easy to type or user keyboard patterns

Hints for good passwords:

- Use phrases or run words together
- Substitute special characters for common letters
- $0methingeasy2remember

19. Malicious Code
    - 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
    - Malicious is anything that could potentially disrupt the normal processing of a computer system.
    - Be careful of websites or applications that ask to load software on your machine.
    - Something as non-threatening as a weather notification tool could be used as an attack vector
    - Unknown and un-patched software could be exploited
    - If you need software to perform your job duties – contact your supervisor or agency IT staff to help you install the software.

20. Email/Email Attachments
    - Email is NOT a secure method of communication except within LEO or MSHP (LAN)
    - As a general rule, don't send anything in an email you don't want others to see
    - Do not send CJI information in an email unless you know the proper technical controls are in place – encryption and access control
    - All email should be scanned for known viruses and spam but it is still an easy avenue for malicious code
    - Virus/Spam detection is only as effective as the latest update
    - You are the last defense in protecting our environment
    - Do not respond or open emails from unknown senders
    - If something doesn't look right, it probably isn't legitimate

21. Internet Policy
    - Internet should be monitored and controlled
    - All devices that connect to the Internet should be protected by a firewall

22. Social Engineering
    - Social engineering is the attempt to gather information by deception
    - Scams and phishing attempts are the major categories of social engineering
    - Social engineering could come from any source – email, telephone, face to face.
    - It won't be obvious the person is trying to gather information
    - Could be masked as a marketing call
    - If you are suspicious – do not answer – report the incident
    - Never respond to an email asking for personal or confidential information, especially if it comes from someone you do not know

23. Laptop/Handheld/Personal Devices
    - There are many personal and work related devices available - know your agency's policy on using these devices
    - Personal devices are not allowed to access CJI Systems
    - Devices need to be secure and managed by the agency's IT staff
    - Need to be password protected and encrypted
    - If lost or stolen, report it as an incident
    - Laptops must be encrypted
    - Laptops/desktops will be managed by IT department to ensure proper controls are in place
    - Agency equipment should not be used for personal uses
    - Do not load unapproved software on any devices
    - Be aware of screen location – avoid shoulder surfing – use screen savers when possible
    - Lock computer before stepping away
    - Use of personal equipment is not allowed to connect to CJIS networks
    - CJI information shall not be stored, accessed or viewed from personal computing equipment
    - CJI information shall not be accessed from library, school or hotel computers

24. Access Requests
    - The access request process 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, if you have least level of access, the less information is at risk
25. Mobile devices
    - Devices cannot be “rooted” or “jailbroken”
    - CJI is only to be transferred between CJI authorized applications on the device
    - Report if the device is lost, stolen, or compromised
      - Include the lock state of the device
      - Include if there are capabilities for remote tracking or wiping of the device
    - Must have a password to unlock the device

Summary

- Information needs to be protected from creation to destruction
- Be aware of information flow – be aware of whom you provide information to - you may pass it to a legitimate person but they may not understand the policy and pass the information to others who are not authorized to have the information
- Providing too much information may allow misuses of the information
- Make every reasonable effort to protect the information 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

Noncompliance

Misuse of official information. 576.050.

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.

Misuse of official information is a class A misdemeanor

I agree that I have read the Security Awareness Training material that was provided to me. I understand what I have read and I do not have any questions. I agree to abide by the rules and regulations as outlined in the Security Awareness Training material.

_____ _____

Signature Date

_____

Printed Name

_____ _____

Agency Name ORI