Kevin Neal <kevin.neal@marshallcountyky.gov>

Special Projects Crew

1 message

misti drew <misti.drew@marshallcountyky.gov> Fri, Aug 26, 2016 at 1:31 PM
To: Kevin Neal <kevin.neal@marshallcountyky.gov>

Judge, I received the letter from Desiree regarding secure areas and personnel access. As it pertains to dispatch, the only member of the crew that would not be allowed in dispatch, per NCIC guidelines, would be We have shared this with you and Gary Teckenbrock previously, but I just wanted to make sure I responded to your request in writing as you directed. The special projects crew has done an outstanding job over here thus far - has not performed any of the work in our center.
If you need anything further, please let me know.

--
Misti Drew
Marshall County E911 Director
50 Judicial Drive, Benton KY 42025
270-527-4733

Marshall County Sheriff's Office

Kevin Byars
Sheriff

August 26, 2016

Dear Sir,

In regard to the Special Projects Crew, I have spoken to Gary Teckenbrock about the situation with one of the members of his crew. This is not to cause a hardship on anyone and this is not personal, personal was over when the law suit was dismissed against myself and others.

My office has sensitive information and has areas that the general public does not have access to without a Deputy being in their presence. The only time a felon is allowed in those areas is if they are being detained and a deputy is with them. Therefore, I am not in favor of that individual being in my office for any reason, unless he has a complaint to be filed or he is an arrestee. Either way a Deputy will be with him in the scope of his duties. Otherwise I do not have the man power to stand and watch him work to make sure everything is secured. Also, the licensing for LINK/NCIC is held by the Sheriff's Office and by Federal mandate a felon cannot be in the same room as the information terminals. The work that is done in E 911 is vetted and anyone that has access to that info, Law Enforcement included, has to pass a background investigation by KSP. The Judicial Building is under the Chief Justice of that center. Judge Mattingly has stated that no one without proper credentials can be in secured areas of the building as well. That is his call not ours.

I do think the Special Projects Crew does very good work. The vetting system used for E 911 will do for my Office as well, If they are allowed in E 911, then they will be allowed in my Office as well. If you have further questions, do not hesitate to call me.

Sincerely,

R. KEVIN BYARS
SHERIFF

RECEIVED
AUG 29 2016
MARSHALL CO. JUDGE'S OFFICE

52 Judicial Drive • Benton, Kentucky 42025
Telephone: (270) 527-3112 • Emergencies: 911 • Fax: (270) 527-4759

5.2 Policy Area 2: Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

5.2.1 Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.

2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.
3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

5.2.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training
A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

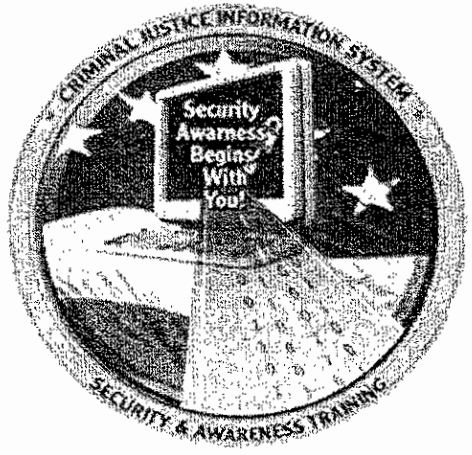
Use Case 4 – Level Three Security Awareness Training
A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing

Example

Criminal Justice Information System
Security & Awareness Training



This is to certify that

BRADLEY WARNING

has successfully completed the CJIS Security & Awareness Course

by completing the following exam:

Level 1 CJIS Security Test

This certification expires two years from the date of issuance.

April 8, 2016		**April 8, 2018**
Certification Date		Expiration Date

Example