A MINI TRAINING SESSION FOR LOSS PREVENTION

Quick Take on Data Security

Data Storage and Destruction

TRAINING OVERVIEW AND OBJECTIVES

Overview: Covers the importance of secure storage and destruction of sensitive data

Purpose:
- Reminds employees about the hazards of unsecured storage and destruction of sensitive data.
- Provides methods to store and destroy data securely so as to prevent data breaches and system intrusion.

Preparation:
- Read and become familiar with this Quick Take. *Change as needed to reflect procedures and personnel in your department.*
- Review applicable policies within your organization and update this Quick Take to reflect those.

Handouts: Quick Review of Data Security—Data Storage and Destruction

Data Security Hazards

Although many hacking attempts are electronic, sometimes people actually come to a location to attempt to gather private information or install devices. This is one of the reasons we have special guidelines to follow regarding secure areas or when destroying private or valuable information. [*Instructor Prompt:* Ask participants for examples of private or valuable information that may be used in their work.]

Numerous cases exist where unauthorized individuals stole or accessed private information without authorization. Local government entities are one of the main targets of hackers. They seek to steal citizens' or employees' personal information, to cripple IT systems for ransom or potentially to affect election results.

IT professionals work to protect systems, but it takes all of us doing our part to keep our systems and data secure. Please pay attention.

Data Storage and Destruction Best Practices

To help prevent unauthorized access to the facility and to sensitive or private data, follow these best practices:

- Do not allow persons without a badge, key or keypad code into restricted areas even if the individuals are known to you. This includes other employees.
- Whenever possible, do not remove any private or nonpublic data from secure storage areas. If you need to remove items, make sure you follow appropriate security policies.
- Visitors, contractors and vendors in a secure area should have an ID, escort or both. [*Instructor Prompt:* Review applicable policies regarding visitors and secure areas with team.]
- Whenever sensitive data is at your workstation, it should be stored in locked cabinets or drawers unless you are there.

- When away from your workstation, you should lock your computer or sign out of the system. For a Windows operating system, you can lock the computer by pressing the windows button and letter “L” key at the same time.
- Keep passwords, ID badges, pass cards, keys or other access devices secure or on your person when away from your workstation.
- When destroying confidential, private or nonpublic data, do not simply throw these items into a garbage can. Use a secure form of destruction, such as cross-cut shredders or other means, to render data unrecoverable. Depending on the type of data, a certificate of destruction may also be necessary to confirm its destruction.
- For mobile or electronic devices, begin data destruction by manually deleting sensitive items and resetting the device to factory specifications or turn the item in to IT specialists to remove the necessary data.

Discussion Questions

- How else can we best maintain secure areas?
- If you are not sure of whether or not an item should be destroyed, what should you do?

Data Storage and Destruction Session Planning and Review

Trainer	Training Date
Department(s)	

TRAINING GOALS

- Refresh employees about the importance of maintaining secure areas and secure destruction of data.
- Refresh employees about best practices to maintain good physical data security and destruction.

RESOURCES

- "Guidelines for Media Sanitation (Publication 800-88 Revision 1)," National Institute of Standards and Technology, NIST.gov
- "Protect Private Data on Copier Hard Drives or Pay the Price," Minnesota Counties Intergovernmental Trust, MCIT.org/resource/
- "Data Backup Options," United States Computer Emergency Readiness Team, Department of Homeland Security, US-CERT.gov

REVIEW

Did the training meet the stated goals?

How can the training be improved?

TRAINER COMMENTS

Attendance Record

Training Session Data Storage and Destruction

Trainer Training Date

Participant Name (printed)	Participant Signature