

Topic: Confidential Information

Date: _____

Trainer Checklist

Task	Date Completed
1. Print Trainee Checklist, fill in employee names.	
2. Review objective and training materials on the confidential information web page at https://sites.google.com/site/kissatisat/topics/confidentialinformation .	
3. Choose one or more methods for employees to learn about confidential information.	
4. Communicate requirement to employees to complete training.	
5. Verify employees can demonstrate knowledge of proper handling of confidential information.	
6. Document employee progress on Trainee Checklist and/or ISA Training Checklist.	

Topic: Confidential Information

Date: _____

Trainee List

Employee Name	Supervisor/Department	Trainer Initials
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		

Lesson Plan

Objective: Demonstrate knowledge of proper handling of confidential information

Limit employee access to data and information

1. When giving access to data, ensure the least privileges are assigned.
2. Provide access to only the system or information required doing a job. This helps to avoid insider abuse.
3. Segregation of duties should be followed while assigning roles and responsibilities. For example, an employee initiating a transaction should not be allowed to approve it as well.

Source: *Small business information security workbook, version 2.2*. Lincke, 2011.

Teaching tip: Ask the participants to name examples of confidential data and material and to describe what should be done to secure them.

1. Dangers
 - a. An individual that was passing by could quickly and easily steal documents left on a desk or another insecure location.
 - b. Sensitive data that is not shredded can easily be picked up by an outsider by simply going through the trash.
2. Confidential data and material
 - a. Any piece of information in any form that contains personal or sensitive information pertaining to any person or entity.
3. What you can do:
 - a. Lock up or destroy any confidential information when leaving your workstation.
 - b. Do not let unauthorized individuals view confidential information.

Discussion point: Ask the participants if they have seen any instances of information not being handled properly.

Note: The material contained in this lesson plan was adapted from the case study "Awareness and Accountability in Information Security Training" (Mellor & Noyes, 2005) and used with permission.

How To

- How to Keep Your Personal Information Secure - <http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure>
- Safeguarding Your Data - <http://www.us-cert.gov/ncas/tips/ST06-008>

Topic: Confidential Information

Date: _____

Lessons

Title	URL	Duration
InfraGard Awareness Information Security Awareness Training Course – Lesson 11 Protecting your workplace from identity theft	https://www.infragardawareness.com	6 Minutes, 50 Seconds
NIH Privacy Awareness Course	http://irtsectraining.nih.gov/publicUser.aspx	30 to 60 Minutes

Tutorials

Title	URL	Duration
Protecting Personal Information: A Guide for Business (interactive tutorial)	http://business.ftc.gov/multimedia/videos/protecting-personal-information	