

Welcome

UF IT Security Policy Workshop Worksheet 2005

Match the correct answer with the questions below.

Questions

- ___ 1. What is a policy?
- ___ 2. What is a standard?
- ___ 3. What is a procedure?
- ___ 4. With whom should IT workers consult to resolve conflicts?
- ___ 5. How much time is allowed to acknowledge incident notifications?
- ___ 6. How much time is allowed for containment of incidents?
- ___ 7. What does DMCA stand for?
- ___ 8. If a DMCA counter-claim is filed, what is the maximum length of time before the material must be returned to service?

Answers

- A. same business day
- B. 10-14 business days
- C. goals or mandates to cultivate standards
- D. Unit ISA & Unit ISM
- E. detailed steps to implement standards
- F. Digital Millennium Copyright Act
- H. metrics used to evaluate policy compliance
- I. immediately, but no later than 24 hours

Please circle Yes or No to the following questions:

10. Do you have systems in your unit that are managed by business associates? Yes/No
- Have they signed agreements? Yes/No
11. Does your unit have external network connections, such as modems? Yes/No
- Are they registered with Network Services? Yes/No
12. Is network space used by personally managed computers protected? Yes/No
- How? _____
13. Do you have critical IT systems in your unit? Yes/No
- Are they registered with Network Services? Yes/No
15. Do you help regularly report security status to your unit administration? Yes/No
16. If a DMCA complaint is not valid do I not have to investigate? Yes/No

more on back....

Take-Away Questions

Please answer the following questions. These are items that UF IT workers should be aware of. If you are unsure what the response is, please seek out the answer or contact ufirt@ufl.edu.

Who is your Unit ISA? _____

Who is your Unit ISM? _____

What are the three most important aspects of securing UF IT resources? _____

What types of incidents must be reported to law enforcement? _____

What should you do if law enforcement requests information from you? _____

What should you do if the press requests information from you? _____

What type of authentication is used in your unit? _____

- Authorization? _____

What methods of access control or firewalls are used in your unit? _____

- Where are they documented? _____

How does your unit manage software licenses to ensure compliance? _____

- Who do you think is legally liable for violations? _____

What code review and/or testing procedures are used in your unit to ensure security of applications? _____

What are the change management procedures for your unit? _____

- Where are they documented? _____

- Do they include vetting of vulnerabilities and patches? _____

Who in your unit is responsible for incident response? _____

Who is notified when students violate policy or law? _____

Who is notified when faculty and staff violate policy or law? _____

What physical protection is used for IT resources in your unit? _____

- Where is this documented? _____

When was the last risk assessment conducted in your unit? _____

- What were the recommendations? _____

- Were they implemented? _____

Are there IT workers in your unit that have not attended IT orientation? _____

- What training opportunities are available to IT workers in your unit? _____

Does your unit have an ITCOP?

- Where is it located? _____

- When was it last updated? _____

- When was it last tested? _____

- Does it include coordination with UF EMS and other campus services? _____

We hope this worksheet was useful. Please feel free to contact us regarding security issues: ufirt@ufl.edu
Thank You!