

# Recommended Answers to Specific ISAAC Questions

## Confidential Assessments

**NOTE** for all Assessments: If any question in ISAAC does not apply (e.g. Are confidential data files encrypted on portable systems? And you do not have portable systems) please indicate “Yes” as your response. This action has been approved and recommended by our internal auditors.

- A8. How many users have received computer security awareness training (including administrators)?
- The Intro field should be equal to the total number of users identified above
- B4F. Please indicate the frequency in which you conduct vulnerability scans.
- Vulnerability scanning is performed by IT Security
  - The response should be Bi-Annually
- B4j. Are new systems secured before connecting them to the TXSTATE network?
- If the standard workstation image is used, this should be answered “Yes”
- B5b. Has the information system(s) owner determined the information asset's value?
- The ISAAC questions ranking Confidentiality, Integrity, and Availability are one form of determining an asset's value
- C5. Are copies of mission critical data stored off-site in a secure, environmentally safe, locked facility (a locked room or container) accessible only to authorized personnel?
- If assessment is for a file share and the file share is located in the data center, then the assessor should answer “yes” to this question
- C8b. Is all mission critical and/or confidential information identified and documented (e.g., ISAAC-S Resource Registration module)?
- If the Device Registration has been completed for this system, then this should be answered “Yes”
- C12. Are security incidents (such as suspected intrusion, illegal activity, or unauthorized activity) promptly investigated, documented, and reported in accordance with TAC 202 security incident reporting requirements?
- IT Security investigates all incidents according to the DIR requirements
- C15. Have all users of the information resources had annual information security awareness training?
- IT Security performs annual security awareness in a variety of venues; semesterly instructor-led classes; security information lists; security website; compliance training; Cyber Security Awareness Day; communications from IT Security
- C20. Does new employee orientation include awareness of information resources security policies and procedures?
- IT Security provides mandatory NEO II security training to all new employees
- C38. If wireless access points are used, are adequate encryption (e.g., VPN or WEP/WPA) and authentication (e.g., RADIUS server) mechanisms in place to secure the wireless transmissions?
- There is an encrypted wireless network on our campus (WPA) and available to all University users through their NetID