ANNUAL SECURITY PRACTICES

Objective:

To determine if all employees of the department or unit are completing the mandatory review of computing security policies and guidelines at least annually.

Important Information:

Per TAC 202, computer users are required to review computing security policies and guidelines at least annually. Training required of all users, such as the UHS mandated information security training, addresses UHD employee responsibility to review security practices on an annual basis. In addition to the UHS training, users are provided with copies of the UHD IT policy statements as well as the *Network and Information System Password Procedure* as part of the university account request and renewal process.

Potential Impact:

Failure to follow mandated annual security practices potentially exposes the University to allowing inappropriate access to protected information and loss or damage of equipment, and puts the University out of compliance with state regulations.

Helpful Tools:

- UH System Administrative Memorandum:

  07.A.03 – Notification of Automated System Security Guidelines

- UHD Website:

  IT User's Handbook

  Annual Review of Security Practices

  Nars The university Account Request has been changed to Nars Information Technology Forms

- Other(s):

  Texas Administrative Code – Chapter 202 – Subchapter C (TAC 202 C)

  The *Secure Our Systems* training course is available online via the UHS Online Training website at http://www.uh.edu/onlinetraining/. Staff is advised to use this login link; **do not log-in through PASS.**

Contacts:

Jon Garza
garzaj@uhd.edu
713-221-8950
S701

Frequently Observed Weaknesses/Deficiencies:

- Existing staff fail to take annual online training regarding computing security policies and guidelines or newly hired staff fails to take the required mandated training within 30 days of employment.

Best Business Practices:

1. Ensure easy and convenient access to required training.
2. Monitor staff completion of required training during specified window(s).

AREA

This questionnaire is designed so that "no" answers indicate that an internal control weakness may exist and the procedure/process may need to be examined in greater detail. **Comments should be provided for "No" answers.** When such weaknesses are identified, a change in the process may be necessary OR a control may need to be put into place to address the weakness. The appropriate UHD contact office (as outlined in the self-assessment text) may be contacted for assistance with identified weaknesses.

Self-Assessment of Internal Controls for: Annual Security Practices	Yes	No	N/A	Comments
Did all staff review computing security policies and guidelines annually?	☐	☐	☐	
Have all employees completed the mandatory UHS Information Security Awareness training?	☐	☐	☐	
Did all new users receive copies of the UHD IT Policy statements as well as the *Network and Information System Password Procedure* as part of the University account request process?	☐	☐	☐	

This is a living document and will be updated as revisions are necessary. Periodically, you may want to check for updates and revisions. We welcome any questions and feedback regarding the information contained in this tool including any comments regarding how this may be more useful and effective.