CEHD Information Security Procedure
IS-11 Special Purpose Computers

Procedure Statement

Some computing devices serve unique purposes for which standard IT security rules cannot be readily applied. These include situations where a computer is dedicated to running critical hardware or software for which non-standard setups are required or strongly recommended by the vendor.

This procedure outlines guidelines and best practices for these situations.

Official Procedure and Responsibilities

1. For all special cases, due effort should be made to configure the computer to comply with university and college IT security rules. However, if business-related restrictions make this unfeasible exceptions can be made in consultation with the CEHD ISO.

The following options can be considered for special purpose situations.

2. Option. Remove the computer from the network. If a computer is not connected to the network, then the only security threat to the computer or by the computer comes through physical access to the computer.

   2.1 To enact this option on a computer, notify Technology Services with the following information

      2.1.1 serial number,

      2.1.2 AMU #,

      2.1.3 location of the computer (building and room number),

      2.1.4 custodian of the computer (person responsible for the computer),

      2.1.5 will sensitive or confidential data be stored on the computer?,

      2.1.6 and the special nature of the computer. (why does it need to be off-network)

   2.2 Once off-network, the computer cannot be regularly managed by Technology Services. It is the responsibility of the custodian to protect the computer and any data stored on it. The custodian is also responsible to ensure that the computer is not connected (even temporarily) to the network.

2.3 Any data should be added or removed through physical means such as USB drives, CDs, and DVDs. Be sure to use anti-virus protection on any computers who will interact with this data to prevent infection of the off-network computer.

2.4 An off-network computer should never be reconnected to the network (even temporarily) without first discussing with Technology Services. In order to return the computer to the campus network, the computer must be brought back into full compliance with all IT security rules and should be done in conjunction with Technology Services.

3. Option. Depending on the special requirements needed. Exceptions to specific rules might be possible. Some exceptions will require university approval, others could be worked out internal to the college.

4. Option. Obtain administrative authority for the computer. If the special needs of the computer are such that none of the above options work, the custodian can take on full responsibility of the computer. This would include providing a justification to the CEHD Dean and the university as to why the computer should be exempt from particular security rules, create a security plan for the management of the device, and conduct an annual risk assessment. (See https://it.education.tamu.edu/it-security/administrative-authority-request-procedure the process.)

Other Special Situations

5. Non-forced OS updates. If a computer is involved in extended (multi-day) processes that would be disrupted by forced operating system patch updates, the end-user may request an exception from forced updates. For this exception to be granted, the end-user must agree to manage updates manually and Technology Services will have to add the computer to a list of specially reviewed computers to ensure updates are installed within a reasonable period of time (at least once every two weeks).

Last Update. July, 2017