Scope

This policy applies to the College of Dentistry’s policy on vendor supplied systems, including hardware and software.

Policy

All vendor supplied computer systems installed in the College of Dentistry must meet with the following security guidelines. Any system that cannot run under ALL the controls below will not be allowed to be installed at the College of Dentistry.

1. All computers must be fully managed by the College of Dentistry IT department. This includes:
   a. Making the computer a campus “domain” member, subject to SCCM and Group Policy management rules.
   b. Windows updates must be turned on and controlled by Dentistry IT.
   c. The campus standard Antivirus software must be enabled and configured according to Dentistry IT standards.
2. Remote access will not be always available. Remote access will only be turned on when needed, and when Dentistry IT is present to monitor the vendor. Remote access will be disabled when the necessary work is completed.
3. Software must function correctly while logged in as a standard windows user that does not have administrative rights. A domain account is preferable to a local windows account.
4. All vendor account passwords must comply with the University password policy.
5. Systems that do not transmit data off campus will be connected to the local scope network.
6. All vendors must have a signed Business Associates Agreement (BAA) in place if PHI is involved.
7. All vendors must complete the College of Dentistry Systems Assessment Questionnaire before a purchase order will be issued.

Resources

University of Iowa Information Security Framework Policy
http://itsecurity.uiowa.edu/policy-information-security-framework

College of Dentistry Systems Assessment Questionnaire
https://www.dentistry.uiowa.edu/sites/default/files/docs/policies/Systems-Assessment-Questionnaire.pdf