UF UNIVERSITY of FLORIDA Information Technology

Standard: System Security

Purpose:

To specify controls required to secure Information Systems against unauthorized access and use.

Standard:

All Information Systems will:

1. Run current versions of software that is supported with updates and patches as security vulnerabilities and flaws are discovered.

    a. Patches addressing security vulnerabilities should be installed as soon as operationally feasible, according to the following schedule:

        i. For vulnerabilities rated Critical, within 14 days after release by the vendor or developer

        ii. Vulnerabilities listed in the *CISA Known Exploited Vulnerabilities Catalog* by the 'Due Date' listed in the catalog

        iii. As otherwise directed by the UF Computer Security Incident Response Team

        iv. Patches for all other vulnerabilities should be applied within 30 days after release by the vendor or developer. Situations in which security patches cannot be installed within 30 days shall be addressed in a security risk assessment.

    b. For situations in which systems that cannot run vendor supported operating systems are essential, such as computers controlling equipment that the manufacturer has not provided updates for, refer to the *Guidelines for Unsupported Operating Systems at the University of Florida*.

2. Verify a user's authorization before allowing access.

3. Display the following usage notification, or another as approved by General Counsel, prior to granting a user access:

   > Welcome to the Gator Nation!!!
   > You are accessing a University of Florida information system and agree to the terms and conditions of the UF Acceptable Use Policy.

   UF Shibboleth SSO displays this message, and thus applies to any web applications requiring UF Shibboleth SSO authentication.

4. Not provide sufficiently detailed feedback about login failures to allow an attacker to deduce proper login credentials.

5. Be protected against Denial Of Service (DOS) attacks that render a system too busy to fulfill legitimate workloads.

6. Employ mechanisms to protect against malicious software. Malicious software mechanisms are updated frequently to address new threats.

Information Systems that Store, Process or Transmit Restricted Data will:

1. Require re-authentication after a period of user inactivity. The period will vary depending on the risk of unauthorized physical access, but typically will not exceed 30 minutes.

2. Protect the confidentiality and integrity of data transmission.

3. Employ mechanisms to detect unauthorized changes to software and information.

4. Employ encryption of data at rest or implement appropriate compensating controls.

References:

CISA Known Exploited Vulnerabilities Catalog

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Guidelines for Unsupported Operating Systems at The University of Florida

https://it.ufl.edu/media/itufledu/documents/policies/networking/guidance-doc-upsupported-os-at-uf.pdf