THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy:
IT0134-M-E - System and Communication Protection Program Exceptions

Version: 1	Effective Date: 08/05/2019

MEMORANDUM

Date: July 3, 2019
From: Amy Belew, CIO, Information Technology Services
Subject: Policy IT0134-M

I acknowledge we are currently non-compliant with implementing DNSSEC according to policy IT0134-M and I accept the risk. We have the following mitigating controls in place:

- Servers only respond to internal DNS requests
    - Restricts access to devices on the internal network
    - Ensures that external parties cannot access internal DNS information

- OS logs sent to SIEM for monitoring
    - Logs are stored in the SIEM for historical and investigatory purposes
    - The logs can be reviewed for anomalies, if needed
    - Correlation rules in the SIEM help identify issues

- Malicious code protection
    - Protects the DNS servers from malicious software
    - Anti-malware is managed by SCCM and email alerts are configured

The following shows our plans for becoming compliant:

- Research and testing – in progress
    - We will research the methods and implications of implementing DNSSEC in the environment
    - If able, we will work with test machines to develop and test procedures
    - Also use this to develop and test roll back procedures in case of major issues

- Enable DNSSEC in the environment – January 2020, depending on results of research and testing