The University of Texas
Rio Grande Valley
Information Security Office

Dear UTRGV Community,

In coordination with Federal, State, and University officials, UTRGV has been implementing various defensive measures to help protect the institution and reduce our vulnerability to Apache Log4j, a recently discovered large-scale vulnerability affecting billions of devices worldwide. At this time, these measures appear to have protected our systems from attack.

There are numerous indications that cyber-attackers are looking to exploit these vulnerabilities further as patches to the vulnerability become available. Because of this, we will need to begin installing patches, fixes or implement other actions to protect our University's systems and data. Safeguarding our technical infrastructure will require rebooting some servers or restarting some services. While we will make every effort to post notifications about these reboots and restarts, some reboot requirements will be unknown until the patch is loaded. When system interruptions are known, these updates will be posted in the UTRGV Messenger. Please know that applications can become unstable after installing a patch, though we will make every effort to ensure this does not happen. That said, if you experience any issues after rebooting the patched device, please contact the IT Service Desk.

Additionally, there are some applications where patches, or fixes, are not available or go undeveloped by vendors. In these cases, it may become necessary to isolate or remove these vulnerable applications or systems to prevent or minimize damage from a cyberattack. While ideal solutions will avoid these potential disruptions, please know that situations requiring quick actions may arise. If you have any questions or concerns, please contact the IT Service Desk or the Information Security Office.

Thank you for your cooperation and understanding as we work through this security issue.

Sincerely,

Information Security Office & The Office of the CIO

UTRGV™