LOCAL FIREWALL POLICY FOR SERVERS AND WORKSTATIONS

INTRODUCTION

All University of Arkansas at Pine Bluff's Servers and workstations should be running a local firewall.

I. WORKSTATION FIREWALLS

    a. All UAPB workstations should be running a local firewall. The UAPB default is the firewall that comes installed with the operating system, whether it is Windows or Mac. The policies are set via Active Directory group policy.

    b. Smart devices that do not come with a firewall installed with the OS, or do not have viable firewalls on the open market, are exempted from this policy.

II. SERVER FIREWALLS

    a. All UAPB Windows servers should be running a local firewall for instance "Windows Firewall"

    b. All UAPB Linux/Unix servers should be running a local firewall such as "IP tables"

    c. If a firewall is turned off for testing, the firewall must be turned back on after testing is completed

    d. In rare cases where a firewall is causing issues and keeping a server from functioning, it may be turned off at the discretion of the Director of Technical Services, after consultation with Server Administrator, and the software vendor. However, all efforts must be made to get the server application working with the firewall, including consultation with the vendor.

REFERENCES AND RELATED DOCUMENTS

Researched on the internet and reviewed various Universities' policies online.

POLICY DOCUMENT INFORMATION

Continuous improvement. The content of this document subject to regular review based on input from UAPB Technical Services staff and the campus community. Suggestions for improvement should be directed to the Director of Technical Services.