Introduction
Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data confidentiality, integrity and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are in compliance with 1_180_Server Hardening Policy to prevent unauthorized access, unauthorized use, and disruptions in service.

Purpose:
Servers at Texas A&M University-Kingsville play an important role in the delivery of critical data to students, faculty, staff, and the public. To this end, controls must be in place to protect the confidentiality, integrity, and availability of the data housed on these servers. Technical, Managerial, and Operational controls work together to assure that new servers are installed and configured in such a manner to emphasize security and minimize service disruptions. These requirements are outlined in this policy and collectively define the university’s required server base configuration.

Policy:
All servers connected to the Texas A&M University-Kingsville network must meet the server hardening requirements outlined in the 1_180 Server Hardening Policy. Servers which process, transmit, or store sensitive data may have additional requirements. All server purchases must be approved by iTech.

Once a new server has been configured to meet the university required hardening standards, the primary administrator should complete the static IP request form. Prior to a new server entering production status, a security scan of the system must be completed by iTech. Identified risks will be communicated to the system administrator and must be corrected or justified.

Disciplinary Actions:
Any servers connected to the Texas A&M University-Kingsville network, found to be in violation of the TAMUK New Server Policy will be disconnected from the network without notice. Failure to comply with this policy may result in disciplinary action.